



CionSystems provides a software management suite that fills critical gaps in Microsoft Azure, Office 365, Microsoft Exchange and Active Directory (AD) and other non-Microsoft LDAP/Directory, OpenLDAP, Linux, Google, Salesforce, IaaS clouds, and SaaS offering. We provide a full range of operations, Identity & Access Management, and enhanced security. CionSystems' solutions allow businesses to effectively, efficiently and economically manage security – for both on premise and off-premise systems, applications, and data. The software management suite consists of several distinct software modules that can be used independently or in any combination depending on the needs of each customer. These modules are described in detail below.

IDENTITY & ACCESS MANAGEMENT FOR ON-PREMISE AND OFF-PREMISE, HYBRID, CLOUD ENVIRONMENTS

ACTIVE DIRECTORY MANAGER PRO

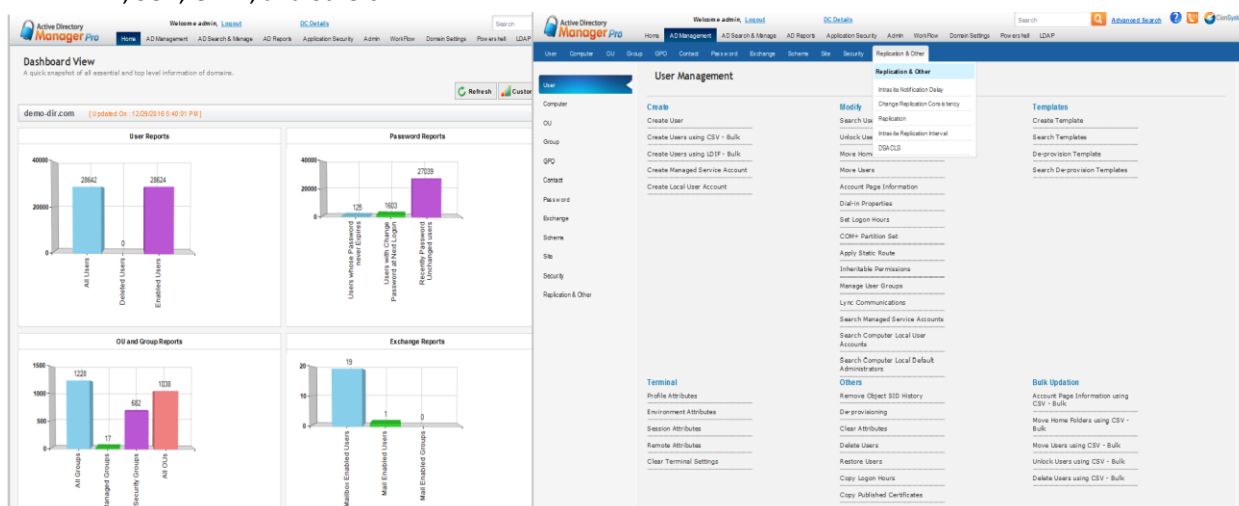
Active Directory Manager Pro is CionSystems' flagship product that provides full management of the data and information contained within an enterprise's Active Directory environment. Unlike the Microsoft Management Console (MMC) snap-in for AD, CionSystems' AD Manager Pro provides a rich, web-based graphical user interface that can be securely accessed using any browser from anywhere on the network: on premise or via secure remote access methods, such as HTTP/S or virtual private networking (VPN).

AD Manager Pro allows I.T. staff to delegate administration across various security administrators, business units, or other delegation models, which is a key gap in Microsoft's rudimentary tools. In addition, it supports workflows and approval processes for provisioning and access requests. The combination of secure browser access, delegated administration, and workflow capabilities solve several key problems that are not addressed by native AD tools:

- Minimize human interaction (and therefore, human error) for repetitive, routine, or complex tasks using built-in automation, all without the requirement of heavy coding, customization, or scripting
- Create, read, update, and delete all objects managed within AD (users, organizations, resources, groups, policies, etc.) using single operations via the browser user interface, or in bulk operations by batch import
- Control by role what objects and functions various delegated administrators are allowed to access and invoke within AD Manager Pro
- Securely manage users, their group memberships, their attributes, and their permissions to applications, SharePoint, files, printers, etc. across multiple domains
- Support for complex, multi-stage workflows and approvals
- Automated provisioning of AD accounts, including Microsoft Exchange mailboxes, and SharePoint and file/print permissions using the optional provisioning module



- Better security by providing a centralized application for managing administrative access without requiring complex cross-domain trust agreements or direct console access that are required when using native AD tools
- Built-in dashboard view of AD health
- Over two dozen built-in reports covering General User Reports, Account Status Reports, Logon Reports, Group Reports, and Service Account Reports, satisfying audit and compliance requirements such as HIPAA, SOX, GLBA, and others.



BENEFITS

- Lower cost of operation
- Centralized access, single point of access
- Fast, automate user provisioning
- Full reporting and auditing
- Enforce policies and prove compliance
- Reliably manage access rights
- Helps with migration efforts
- Easy install and ramp-up
- All functionality included in one file, no need for multiple modules
- Task approvals decrease errors and inconsistencies
- Automates the provisioning and DE provisioning process
- Schedule the tasks of adding and removing objects
- Monitor the execution of tasks
- Ability to accept or operations deny requests
- Easy compliance and governance - who, when, what, where
- Easy Permission management and determination
- Central management for on premise Active Directory and Office 365

FEATURES

- Browser-based UI, customized by role
- No coding or command line scripting
- Workflow Support
- Robo Request
- Secure provisioning and DE provisioning
- Role Based Access
- 200+ ready-to-use reports, customizable
- Exchange mailbox management
- Centrally manage multiple domains
- Bulk object management
- Customizable templates increase functionality
- Real-time notifications – inbox size, password expiry, etc.
- Change Approval process
- Office 365 Management
- Exchange (2007/2010/2013) Management Through Powershell
- AD Management Through Powershell
- Manage Local Computer User accounts
- Managed Based Service Accounts

- Audit trail - who, when, what, where
- Easy permission determination
- Bulk Modifications management
- Temporary User and Temporary Group and Group membership management
- Schedule object addition and removal-automated cleanup
- Delete Object Archival and Restore
- Granular password, ACL management
- Group Policy Object (GPO) management
- OU Delegation
- Computer, Group, Contact, Site, Schema, Replication, Password management

AUTOMATED USER AND ACCESS PROVISIONING

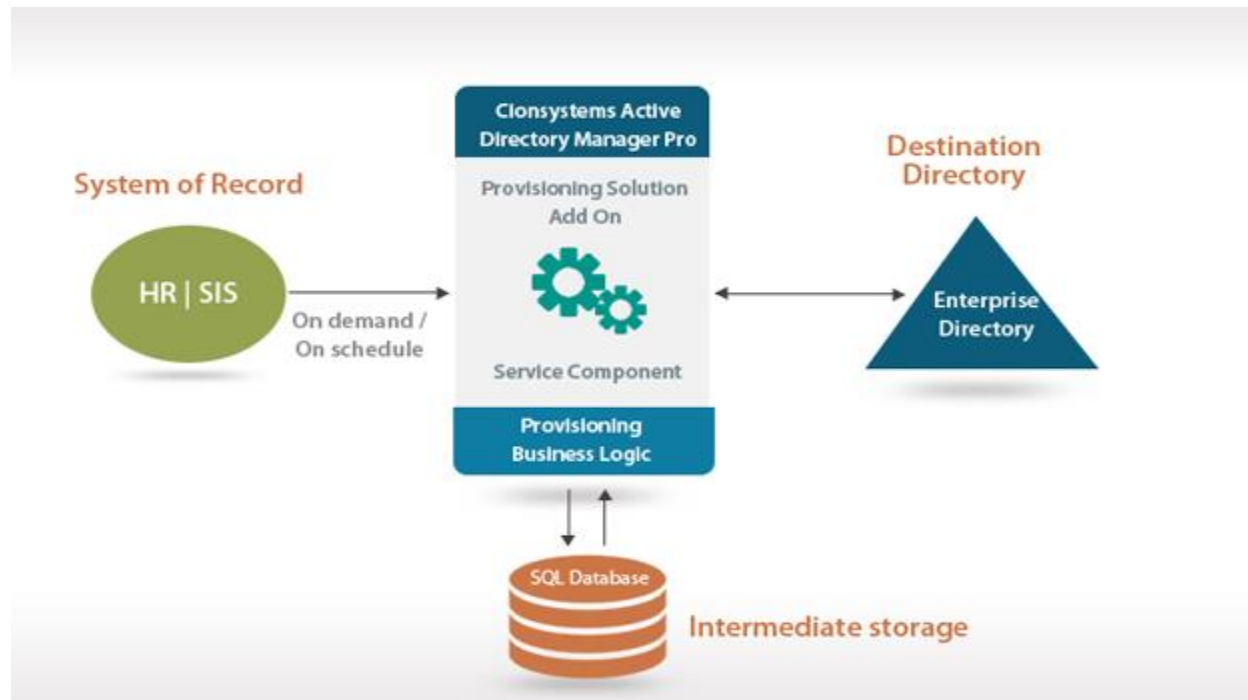
User Provisioning System creates modifies disables and deletes user accounts across IT infrastructure and business applications. Provisioning system use templates and business rules to automate onboarding, off-boarding and other administration workforce processes such as, new hires, transfers, promotions and terminations. Typically the system runs on schedule basis and ensures that data is transferred or provisioned in the destination system from the source while applying rules/policies that transforms the data for destination system.

User provisioning to company software such as enterprise directory, IT-infrastructure commonly known as identity management, has typically been a daunting task for enterprises. Automated user provisioning allows tasks that would normally take days to enter mere hours, creates a single point of failure, while making your environment more streamlined. Automated user provisioning makes the process of user creation, modification and deletion simple, cost effective, secure, efficient and streamlined.

CionSystems provisioning system simplifies this process via their predefined and customizable templates, policies via simple user interface. User provisioning doesn't have to be complex anymore. No script or code is needed.



CionSystems Provisioning system has two major components. First one is a service component which is continuously run on schedule basis, based on the configuration. Second one is user interface to manage the system which is integrated in Active Directory Manager Application under Provisioning Tab.



Provisioning system has features like import supplement/master data, configuration of transactional files schema, other configuration settings, status tracking, audit logging and error logging.

AD CHANGE AUDITOR AND REPORTER

A companion module to Active Directory Manager Pro, AD Change Notifier & Reporter modules provide a granular and detailed means of tracking all changes made to the AD environment that is simply not possible or scalable using the native Event/System/Error logs built into the Microsoft platform. These modules provide full visibility of ALL changes to the AD environment, including domain changes, structural changes to the tree, changes to the schema, changes to Group Policy Objects, and of course, any data changes to objects stored within AD. These changes are tracked in real-time, including the timestamp, source of the change, and the identity of the user who made the change, providing a complete record for auditing and compliance purposes.

While the Reporter module provides enhanced reaction ability in the event of a compliance audit or forensic investigation, the Notifier module allows administrators to configure particularly sensitive activities to be monitored and alerted in real-time to ensure that critical changes like domain structure modification and schema extensions are not allowed outside of change control governance.

Active Directory changes daily, yet most IT organizations are unaware of the changes until something breaks. This leads to downtime, loss of productivity, and higher cost. Becoming proactive and more aware is part of the overall



IT optimization strategy. The Active Directory Change Notifier is an invaluable resource when IT organizations are developing a proactive approach to managing their infrastructure.

- Monitor AD Administrative Activities
- Detects Who Changed What and When
- Real Time Notifications
- Enterprise-class Scalability
- Changes logged for analysis and archiving
- Regulatory Compliance

The screenshot displays the CionSystems AD Change Notifier web application. The left sidebar contains the 'Audit Settings' section with a 'Save' button and a table for configuring monitoring for various AD objects. The main content area shows three 'Active Directory Change Report' summaries for different object types, each with a table of recent changes.

Audit Settings Table:

	Create	Modify	Delete		Create	Modify	Delete
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Builtin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Computer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Computers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Foreign Security Principals	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Organizational Unit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Lost And Found	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Contact	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Microsoft Exchange System Objects	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GPO	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	NTDS Quotas	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Printers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Program Data	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Shared Folders	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
				Users	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Active Directory Change Report Summary 1:

Object Name	Object Path	Object Type	Change Type	Change Date and Time	Changed Details	Changed By
morph.com/MyOU/PC/CN=Faruk10532 Shaik	CN=Faruk10532 Shaik,OU=PC,OU=MyOU,DC=morph,DC=com	user	MODIFY	12/1/2016 12:01:00 PM	Account Status: Disabled GUID: 6c52a938-00fc-43bf-9992-848801046994 Instance Type: 4	Administrator

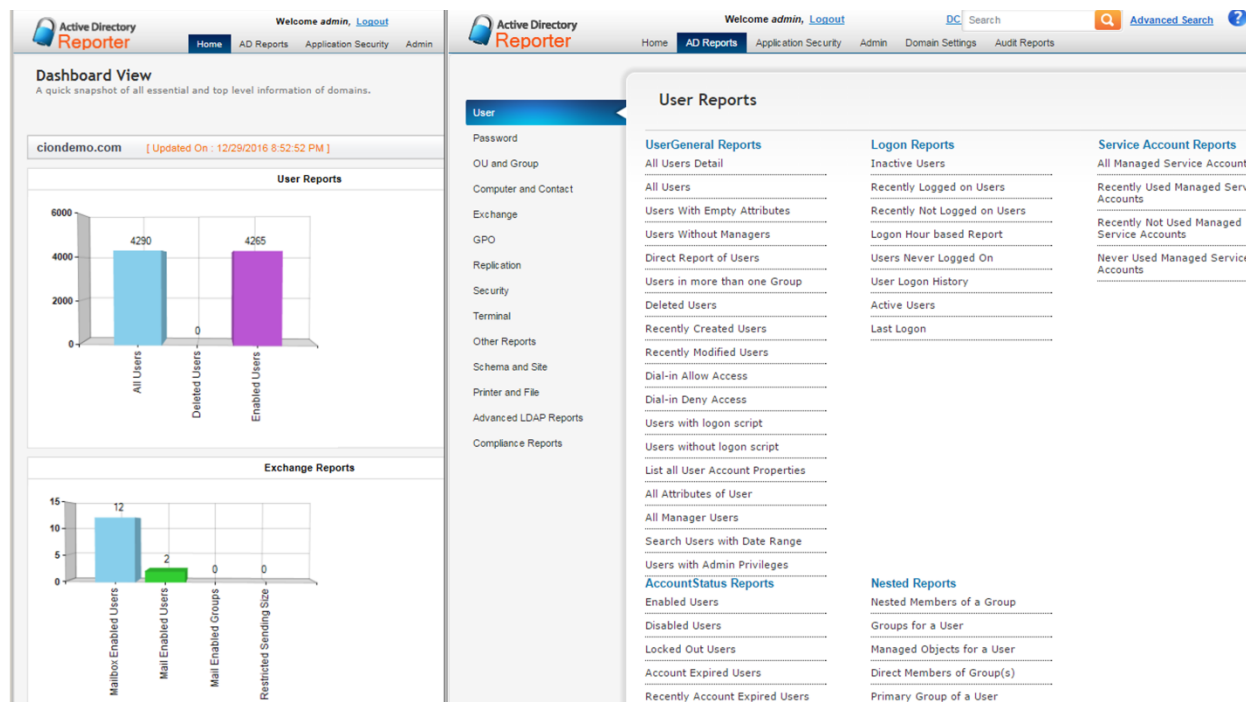
Active Directory Change Report Summary 2:

Object Name	Object Path	Object Type	Change Type	Change Date and Time	Changed Details	Changed By
morph.com/CN=Deleted Objects/CN=Faruk10531 Shaik 0ADE1b7e820de-a00f-442f-997b-9b1f69eb87b2	CN=Faruk10531 Shaik 0ADE1b7e820de-a00f-442f-997b-9b1f69eb87b2,CN=Deleted Objects,DC=morph,DC=com	user	DELETE	12/1/2016 12:05:12 PM	--	MORPH\System

Active Directory Change Report Summary 3:

Object Name	Object Path	Object Type	Change Type	Change Date and Time	Changed Details	Changed By
-------------	-------------	-------------	-------------	----------------------	-----------------	------------

Reports



ENTERPRISE SELF SERVICE

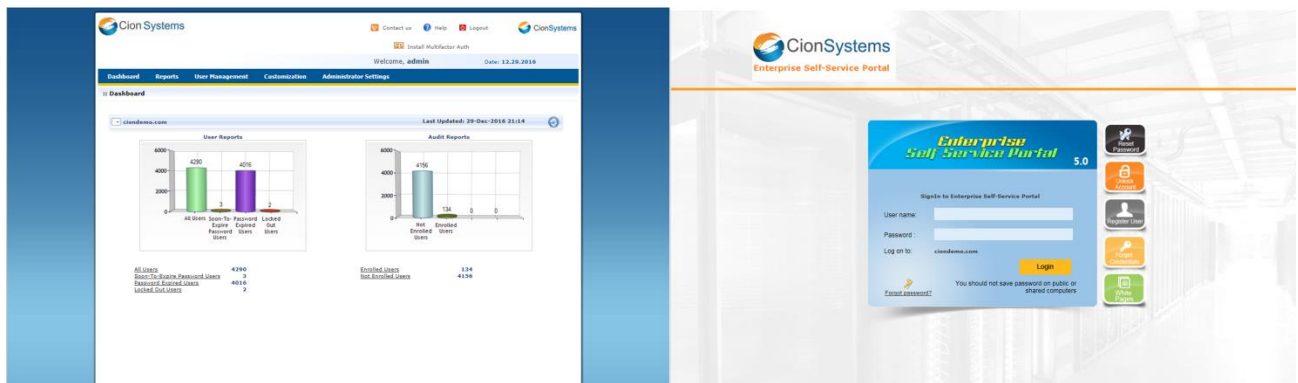
This module builds on the core capabilities of AD Manager Pro, and provides a browser-based interface designed specifically for enabling end users to self-manage certain aspects of their own profile. It also includes self-service lost password recovery and password reset functionality that can help organizations dramatically reduce the most common calls to the I.T. help desk. Password reset and account unlock features can be integrated with the end user's smartphone, tablet, shared workstations, or kiosks. Of course, all user actions follow a defined workflow, and are recorded, which supports audit and compliance requirements.

As with AD Manager Pro, Enterprise Self Service supports both delegation and workflow, and includes the most common delegation model out-of-the-box: super-user, power users, and end users. Other important capabilities of this module include:

- Automated manager delegation and object control, utilizing AD's built-in "manager" attribute
- Complete delegated administration of group creation and membership, including primary and secondary group owners, for both security groups and distribution lists
- The ability to support multiple password policies and associate them with a specific AD domain, organizational unit (OU) within a domain, geography, or even based on group membership
- Can be configured to use CionSystems multi-factor authentication (MFA) solution for improved security, especially for remote access and administrator use cases



- Out-of-the-box self-service password resets for Microsoft AD, OpenLDAP, AzureAD, Office365, Google apps, and Salesforce.com (other sources can be added through configuration)
- Support for password synchronization across multiple back-end repositories, including Microsoft AD, OpenLDAP, AzureAD, Office365, Google apps, and Salesforce.com
- Out-of-the-box “white-pages” application with free-form search for Azure AD, Office365, Active Directory and other connectors



CionSystems allows employees to self-manage their accounts without having to call the Help Desk.

CionSystems Enterprise Self Service product is a state-of-the-art solution for identity administration and access control

Features

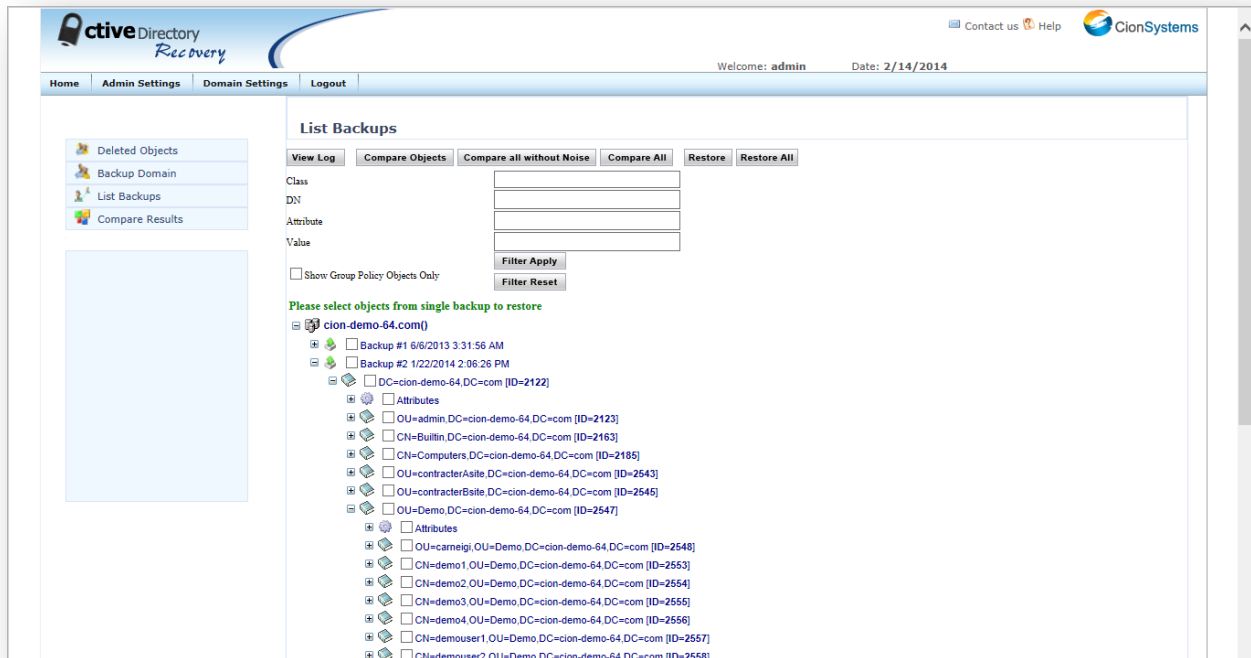
- Password management
- User self-registration and self-service
- Supports Active Directory, OpenLdap, Other LDAP compliant directories, Virtual Directories, Azure AD or Office365
- Supports hybrid or pure cloud environment
- Web based, lightweight footprint
- Simple, configurable three tier access model: administrator, power user and users
- Profile including manager attribute, Contact and Self group membership management.
- Complete group management, supports primary and secondary group owners
- Flexible password policies that can vary based on domain, OU, geography, and group membership
- Enforces strong authentication policies
- Account lock and unlock by administrator or users
- Self-service Password reset, for Microsoft AD, OpenLDAP, AzureAD, Office365, Google apps, Sales force
- Password synchronization between Microsoft AD, OpenLDAP, AzureAD, Office365, Google apps, Sales force
- Web-service API's for integration
- Manager can manage all direct reports profiles
- Delegated user can manage their assigned objects like OU's, groups, users and other objects
- White-pages - free form search for Azure AD, Office365, Active Directory and other connectors
- Full audit support - All changes are tracked including who changed what and when

AD BACKUP & RECOVERY



While Microsoft AD has become critical infrastructure for most enterprises, Microsoft does not provide an adequate tool for backing up or recovering AD data or schema configuration. As more and more applications rely upon AD for authentication and authorization, any outage within the AD infrastructure could have serious detrimental effects on the availability of critical business systems. CionSystems created this important operational tool to enable I.T. administrators to regularly backup critical AD data, as well as a utility that provides for rapid restoration in the event of an outage, data corruption, or other unauthorized change to AD.

Native tools require an all or nothing approach, but often, a granular approach is required, where specific objects – with all of their attributes intact – must be restored. This granular capability is particularly important for recovering Group Policy Objects, which are the backbone of the security model underlying AD (and AD-reliant applications such as SharePoint, .Net applications, or other natively-integrated applications). The granular approach also means that recovery time can be dramatically reduced when compared with the native tool's all-or-nothing method.



- Choose between online Granular Recovery, including object attributes, or Full Domain Restore
- Restore any object including Group Policies in AD, allowing you to recover a deleted user account with all of its group memberships, attributes and password policies without restarting system
- Extensible search capability (deleted item, date, etc.)
- Easily compare backup snapshots or to determine changes between snapshots

GPO MANAGER

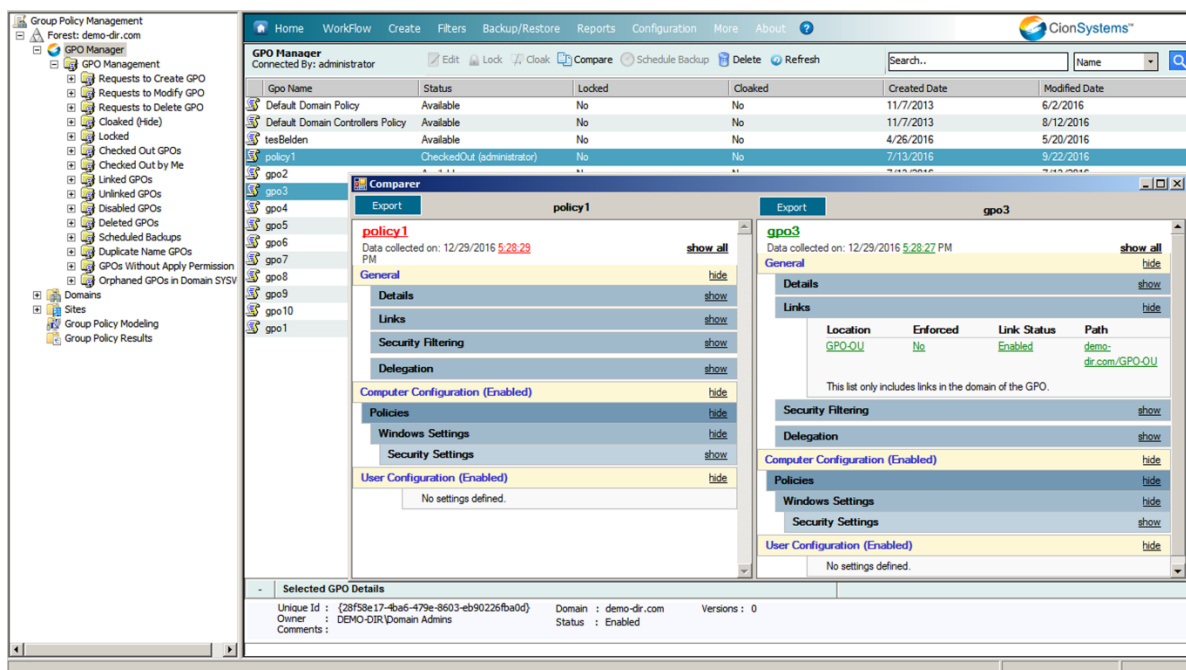
Group Policy Objects (GPOs) are constructs that are stored within Active Directory that allow I.T. administrators to control a wide variety of security settings and access permissions. Examples of how GPOs are typically used include:

- password policies
- allowed logon hours
- what software is allowed on laptops or workstations
- ability to read-write-update directory data
- file and printer permissions

While GPOs are very powerful, the challenge for most organizations trying to manage GPOs with native tools is that they can quickly proliferate to the point of being unmanageable. With native tools, it is common for I.T. administrators to have great difficulty determining exactly what the overall security policy is, and whether or not the GPOs are actually enforcing the policies they were intended to enforce.

CionSystems' GPO Manager provides a robust Microsoft Management Console (MMC) snap-in that dramatically improves the ability of administrators to manage GPOs. GPO Manager provides capabilities not found in the native tools, such as:

- centralized view of tiered and delegated GPOs
- workflow management for policy approval
- policy check in and check out to help manage version control and inadvertent changes
- change control and rollback
- backup and restore
- built-in reports



GPO Manager Benefits:

- Simplifies and automates critical tasks, reduces outages by eliminating manual process and scripts
- Helps prove compliance to ITIL, MOF, SOX, Basel II, HIPAA and C-198.
- Improves availability and disaster recovery via backup and rollback capabilities.
- Simplifies the enforcement of enterprise-wide business policies by enabling streamlined GPO control via workflow.
- Simplifies and improves network security by restricting access to production GPOs.
- Gives Active Directory administrators and security personnel's control of GPO changes, to eliminate system outages and security exposures
- Allows administrators to edit and test GPOs and have them approved before they are deployed
- Archives all GPO settings
- Leverages, complements and extends native Microsoft technology, including Group Policy Management Console (GPMC), to strengthen infrastructure investments

MULTI-FACTOR AUTHENTICATION

One of the most significant security weaknesses in any information system is the password-based single-factor credential that is commonly used to authenticate a user to a system. Security experts widely advocate for replacing single-factor credentials with multi-factor authentication (MFA) methods. While MFA solutions are dramatically more secure due to their ability to withstand brute force, keylogger, man-in-the-middle, and other common attacks, they come with a significant drawback: usability is typically much harder, so consequently, end users often complain about them.

CionSystems has created a user-friendly multi-factor authentication module that can be deployed on managed workstations that utilizes the enterprise's existing username + password credential, and then supplements it with a second factor of authentication. The second factor can be configured for one of three options:

- Token base of Generic USB key
- Offline tokens
- Challenge-Response questions
- Out-of-band PIN sent to email
- Out-of-band PIN sent to SMS / phone



Of course, the MFA solution includes user facilities for selecting their challenge-response questions and managing their email and phone settings. Working in concert with AD Manager Pro, Enterprise Self Service, and GPO Manager, MFA policies can be set on specific objects within the directory (for example, on specific geographic regions, or specific organizational units) in order to enforce strong authentication. For example:

- Require end users to use MFA when accessing highly secure content
- Require administrators to use MFA before accessing administrative functions
- Require users from risky geographic regions

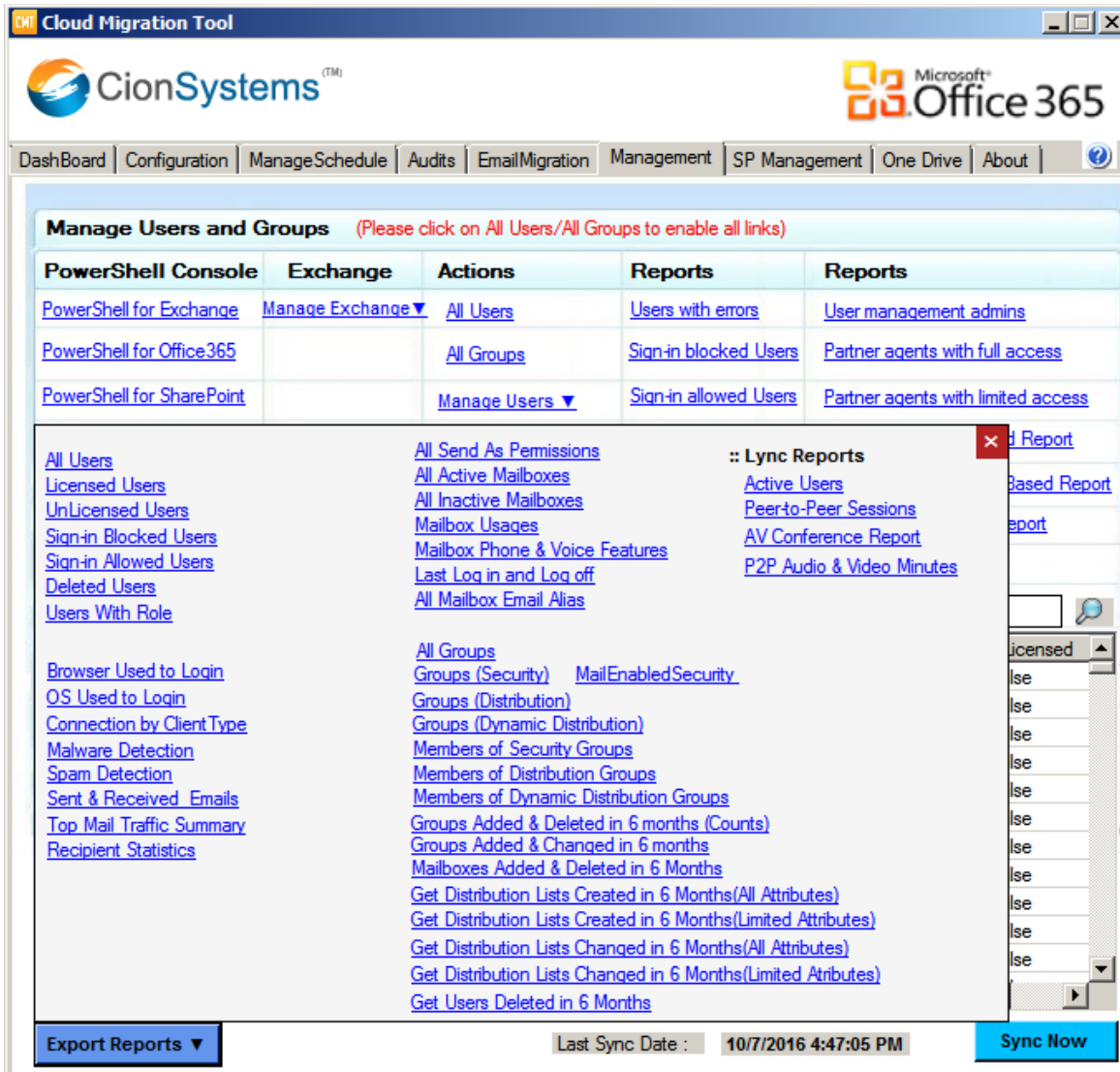
CLOUD IDENTITY MANAGER

For enterprises that have begun to adopt cloud-based services (such as Office365 and Azure-hosted applications), a significant challenge is that security policies and credentials between on premise and off-premise environments quickly become fragmented. O365 and Azure each provide their own identity management facilities, but Microsoft does not provide a single way to manage identities for the on premise AD, the O365 instance(s), or the Azure infrastructure. Consequently, enterprises using both O365 and Azure have to manage the same identity information in at least three places, with the requisite increased management burden and risk of data entry error from manually processing the same kinds of identity information multiple times.



To help ease this burden, CionSystems created a module called Cloud Identity Manager, which centralizes, streamlines, and synchronizes critical identity data between the on premise AD environment and off-premise offerings. Many of the features described in AD Manager Pro are available in Cloud Identity Manager, with the key difference being that the identity information is securely synchronized between the on premise AD and the off-premise management infrastructures at O365 and Azure. Key features include:

- Transparent self-service password management for O365 and Azure users
- Automated user creation and disablement of user accounts in the cloud, minimizing the risk of orphaned users, or users retaining access after separation
- Automated account deactivation based on premise events (typically, account lock or disable in the on premise AD)
- Over two-dozen out-of-the-box user reports not provided by O365 or Azure
- Migration utilities that streamline and phase the migration of users from on premise Office productivity and Microsoft Exchange to O365, including exchange mailboxes or non-Exchange email systems such as POP3 or IMAP4
- Automatic or on-demand deletion of a deactivated user's OneDrive, with automated archiving and migration of data to the manager's share with appropriate access controls applied



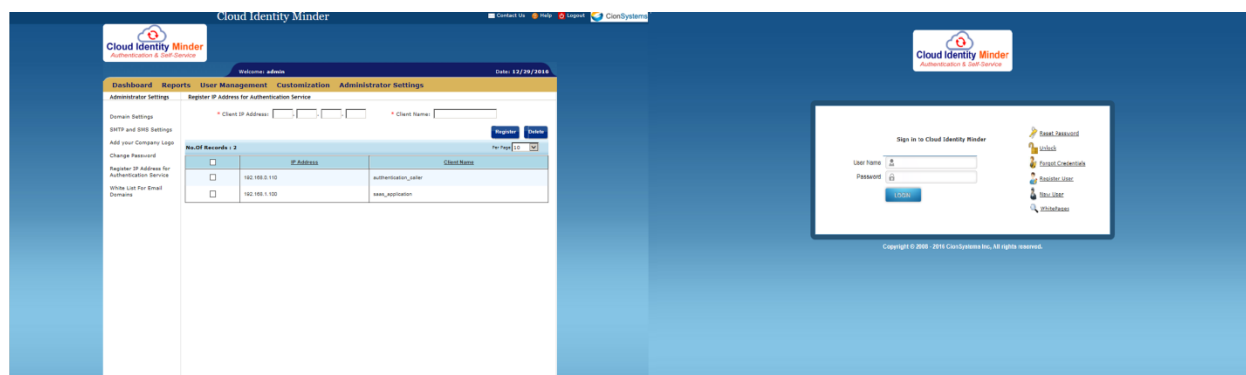
CLOUD IDENTITY MINDER

For enterprises that deploy web applications, another challenge is providing a common authentication experience that is easy to use for end users, while still enforcing the enterprise's required security policies. CionSystems' Cloud Identity Minder is a transparent proxy authentication solution that provides a common, externalized authentication layer that can be used for any web application, regardless of where it is hosted.

The solution provides self-registration for end users (including self-service password management), and the ability to select and request access to applications that may be hosted within the enterprise or at a variety of cloud providers. Once registered, when the user accesses the Cloud Identity Minder landing page and clicks on an application they have been granted, Cloud Identity Minder intercepts the connection and prompts the user to



authenticate. Of course, this capability can be combined with CionSystems' MFA solution to provide strong authentication for higher risk applications.



In addition to the end user interface, Cloud Identity Minder includes a web-based management interface that enables administrators to configure applications, set security policies, perform user administration functions, and other related management tasks. This solution currently supports web applications that authentication to Active Directory, any standard LDAP, AzureAD, and Office365. It also includes a full Application Programming Interface (API) in order to extend the capability to other applications and platforms.

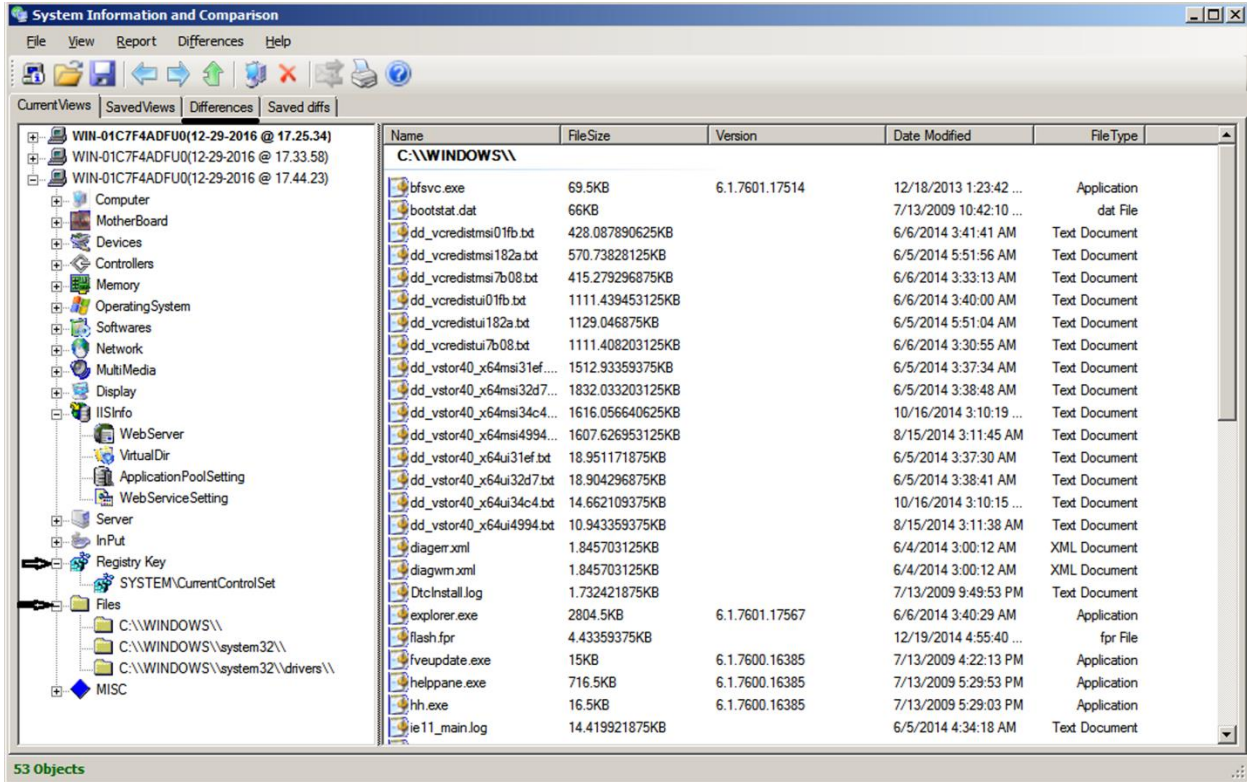
ADDITIONAL MODULES

WINDOWS SYSTEM INFORMATION & COMPARE

One of the biggest challenges faced by Windows systems administrators is identifying the thousands of small but critical changes that occur from the time a system is put into service until the moment it experiences a critical problem. Microsoft does not provide a suitable native tool to be able to identify system level changes on the file system or within the registry, particularly when dealing with a large fleet of servers.

CionSystems' System Information & Compare is a windows-based application that allows system administrators to remotely connect to managed systems, capture snapshots of all of these configuration details, and then perform side-by-side comparisons. The comparison data can be captured locally or remotely, and can be stored on the local system, or in a centralized repository. It also allows administrators to define Master configurations that can be re-applied if necessary, as well as a viewer tool for analyzing changes and pinpointing problems. Since the utility uses the Windows Management Instrumentation (WMI) protocol, there is no need for locally-deployed agents that can

interfere with normal system operations.



The screenshot shows the 'System Information and Comparison' window. The left pane displays a tree view of system components, with 'Files' selected under the 'C:\WINDOWS\system32\drivers\' directory. The right pane shows a list of files being compared, including 'bfsvc.exe', 'bootstat.dat', and various 'dd_vcredistmsi' and 'dd_vstor' files. The table columns are Name, FileSize, Version, Date Modified, and FileType.

Name	FileSize	Version	Date Modified	FileType
C:\WINDOWS\				
bfsvc.exe	69.5KB	6.1.7601.17514	12/18/2013 1:23:42 ...	Application
bootstat.dat	66KB		7/13/2009 10:42:10 ...	dat File
dd_vcredistmsi01fb.bt	428.087890625KB		6/6/2014 3:41:41 AM	Text Document
dd_vcredistmsi182a.bt	570.73828125KB		6/5/2014 5:51:56 AM	Text Document
dd_vcredistmsi7b08.bt	415.279296875KB		6/6/2014 3:33:13 AM	Text Document
dd_vcredistui01fb.bt	1111.439453125KB		6/6/2014 3:40:00 AM	Text Document
dd_vcredistui182a.bt	1129.046875KB		6/5/2014 5:51:04 AM	Text Document
dd_vcredistui7b08.bt	1111.408203125KB		6/6/2014 3:30:55 AM	Text Document
dd_vstor40_x64msi31ef....	1512.93359375KB		6/5/2014 3:37:34 AM	Text Document
dd_vstor40_x64msi32d7...	1832.033203125KB		6/5/2014 3:38:48 AM	Text Document
dd_vstor40_x64msi34c4...	1616.056640625KB		10/16/2014 3:10:19 ...	Text Document
dd_vstor40_x64msi4994...	1607.626953125KB		8/15/2014 3:11:45 AM	Text Document
dd_vstor40_x64ui31ef.bt	18.951171875KB		6/5/2014 3:37:30 AM	Text Document
dd_vstor40_x64ui32d7.bt	18.904296875KB		6/5/2014 3:38:41 AM	Text Document
dd_vstor40_x64ui34c4.bt	14.662109375KB		10/16/2014 3:10:15 ...	Text Document
dd_vstor40_x64ui4994.bt	10.943359375KB		8/15/2014 3:11:38 AM	Text Document
diagerr.xml	1.845703125KB		6/4/2014 3:00:12 AM	XML Document
diagwm.xml	1.845703125KB		6/4/2014 3:00:12 AM	XML Document
DtcInstall.log	1.732421875KB		7/13/2009 9:49:53 PM	Text Document
explorer.exe	2804.5KB	6.1.7601.17567	6/6/2014 3:40:29 AM	Application
flash.fpr	4.43359375KB		12/19/2014 4:55:40 ...	fpr File
fveupdate.exe	15KB	6.1.7600.16385	7/13/2009 4:22:13 PM	Application
helppane.exe	716.5KB	6.1.7600.16385	7/13/2009 5:29:53 PM	Application
hh.exe	16.5KB	6.1.7600.16385	7/13/2009 5:29:03 PM	Application
ie11_main.log	14.419921875KB		6/5/2014 4:34:18 AM	Text Document

Contact:

Zubair Ansari

Cell: (206) 437-1655

Phone: (425) 605-5325 ext 52

Fax: (425) 605-5325

Email: zubair@CionSystems.com