bluechip
infotech

ManageEngine

AD360

Active Directory
最佳整合管理解決方案

藍籌科技
張慶振
Kerry Chang

Helping your business grow

20
YEARS
2020

Celebrating 20 Years with Bluechip

PLATINUM SPONSORS

acer
CyberPower
LogMeIn
SOPHOS

GOLD SPONSORS

EATON
hp

bluechip 與您的企業一起成長

- 總部位於澳洲雪梨，與其他據點
  - 墨爾本
  - 布里斯本
  - 阿得雷德
  - 伯斯
  - 台灣
- 超過101名員工，提供您最佳服務

原生AD管理就夠了嗎？

Native ADUC is not good enough ?

AD管理是一門藝術

- 您是否遇到這些狀況？
  - 權限不容易分配
  - 稽核報表需要花時間整理
  - 常需要幫使用者解決密碼問題
  - 備份還原工程浩大

花費許多心力與成本，卻常常事倍功半

客戶常問的 微軟 AD 管理 Q&A

- 要一次在AD/O365/Exchange新增大量使用者
- 使用者常常要我幫他重設密碼
- 離職的同仁帳號管理
- 主管想要看各種AD的報表
- 稽核想要看使用者行為軌跡
- 想要備份還原AD

AD管理員也是需要被服務的

- 你需要的是：
  - 輕鬆寫意的簡單日常維運
  - 即時有效的狀況預防與感知
  - 更有效率的資安事件處理
  - 節省管理成本

AD360

ManageEngine AD360套件

- ADManager Plus
  - 維運管理和報告
- ADAudit Plus
  - 稽核
- ADSelfService Plus
  - 身份密碼管理與 IT 自主管理
- RecoveryManager Plus(Optional)
  - 備份和復原工具

- O365 Manager Plus(Optional)
- Exchange Reporter Plus(Optional)

ManageEngine AD360管理特點

- 單一管理介面
  - 針對AD/Exchange/Office 365進行管理/報表/稽核/監控
- 細膩的備份還原
  - 屬性/物件層級備份還原
- 即時AD監控/稽核
  - 使用者行為分析、特權群組稽核等等
- 密碼自主管理
  - 大大降低使用者因密碼而無法作業的機率

ManageEngine AD管理同業功能比較

	ManageEngine	Q牌
	AD綜合管理	
透過手機APP管理	可	無法
支援G-suite	可	無法
管理員行為軌跡報表	可	無法
	AD稽核與檔案儲存管理	
使用者工作時數紀錄	可	無法
事件觸發行為反應	可	無法
物件保護機制	無法	可
檔案修改監控	可	無法

#台幣年費計價

ManageEngine AD管理同業功能比較

	ManageEngine	Q牌
AD自主管理		
透過行動裝置重置	可	無法
報告定期自動寄送	可	無法
帳戶到期通知	可	無法
審核使用者變更	可	無法
G-suite/O365 密碼同步	可	無法
備份&還原		
備份/還原物件屬性	可	無法

#台幣年費計價

為何選用ManageEngine AD360

- 少量花費，就能確保AD環境滿足資訊安全規範
  - SOX, HIPAA, PCI–DSS, GDPR, FISMA, GLBA and ISO27001
- 即時監控AD行為軌跡
  - 行為異常將即時回報管理員，並記錄相關資訊
- 整合單一簽入&多因素驗證
  - 支援SAML協定登入，例如Google/O365，支援全景等OTP
- 大幅簡化AD管理
  - 多樣化報表可供查閱，且可輕鬆備份還原

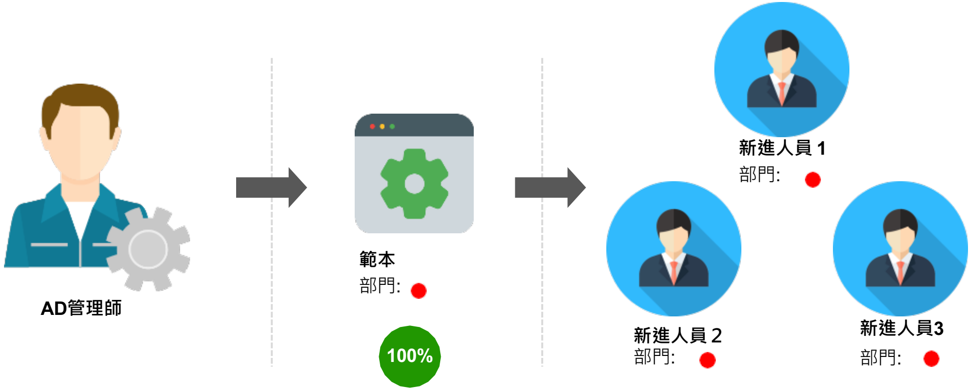
AD360 系統需求

- 需要相對應的AD權限(管理物件/稽核等等)
- 建議硬體規格
  - Processor : P4 – 2.0 GHz or better
  - RAM : 4 GB
  - Disk Space : 40 GB
- 支援平台
  - Windows Server (2019/2016/2012 R2)
  - Windows (10/8)

AD綜合管理

AD綜合管理 – 更方便的人員管理

- 可依照部門或職位，在範本內，設定預設相關權限
- 透過範本部署人員，可有效避免人員設定衝突



AD管理師

範本
部門: ●

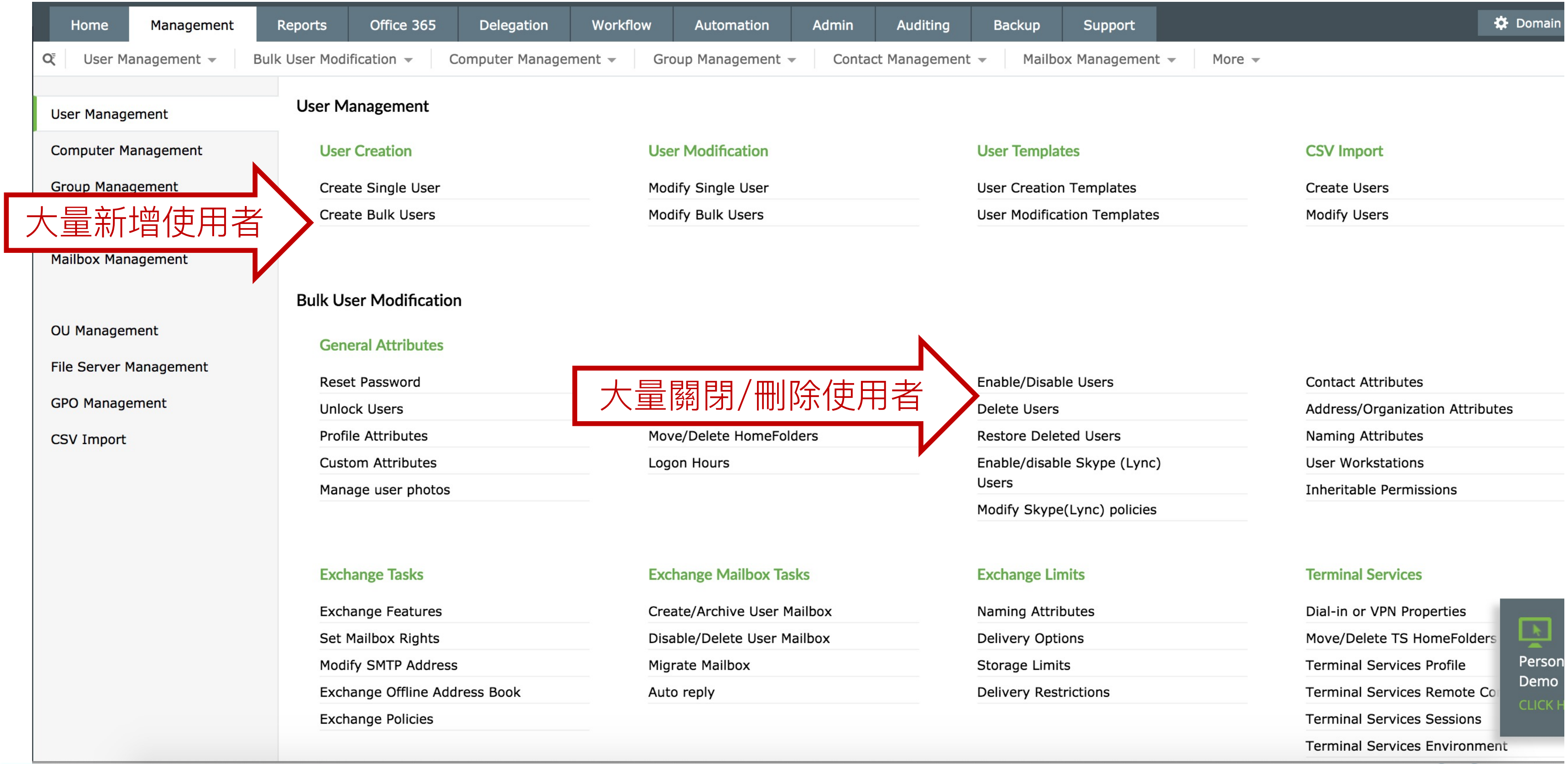
100%

新進人員 1
部門: ●

新進人員 2
部門: ●

新進人員3
部門: ●

AD綜合管理 – 可批次管理


Home
Management
Reports
Office 365
Delegation
Workflow
Automation
Admin
Auditing
Backup
Support
Domain
User Management
Bulk User Modification
Computer Management
Group Management
Contact Management
Mailbox Management
More
User Management
Computer Management
Group Management
Mailbox Management
OU Management
File Server Management
GPO Management
CSV Import
Person
Demo
CLICK H

大量新增使用者

大量關閉/刪除使用者

User Management

User Creation

- Create Single User
- Create Bulk Users

User Modification

- Modify Single User
- Modify Bulk Users

User Templates

- User Creation Templates
- User Modification Templates

CSV Import

- Create Users
- Modify Users

Bulk User Modification

General Attributes

- Reset Password
- Unlock Users
- Profile Attributes
- Custom Attributes
- Manage user photos

- Move/Delete HomeFolders
- Logon Hours

- Enable/Disable Users
- Delete Users
- Restore Deleted Users
- Enable/disable Skype (Lync) Users
- Modify Skype(Lync) policies

- Contact Attributes
- Address/Organization Attributes
- Naming Attributes
- User Workstations
- Inheritable Permissions

Exchange Tasks

- Exchange Features
- Set Mailbox Rights
- Modify SMTP Address
- Exchange Offline Address Book
- Exchange Policies

Exchange Mailbox Tasks

- Create/Archive User Mailbox
- Disable/Delete User Mailbox
- Migrate Mailbox
- Auto reply

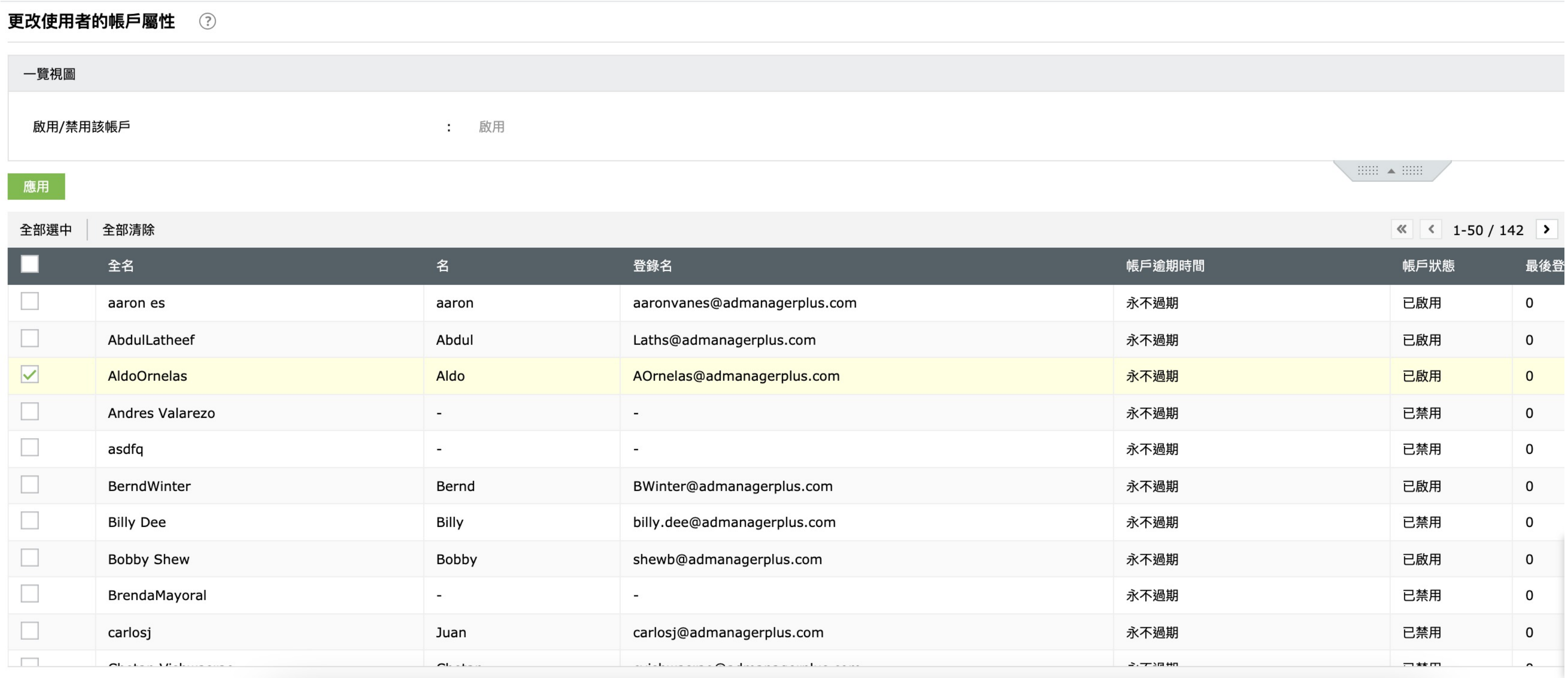
Exchange Limits

- Naming Attributes
- Delivery Options
- Storage Limits
- Delivery Restrictions

Terminal Services

- Dial-in or VPN Properties
- Move/Delete TS HomeFolders
- Terminal Services Profile
- Terminal Services Remote Co
- Terminal Services Sessions
- Terminal Services Environment

AD綜合管理 – 直接勾選大量管理



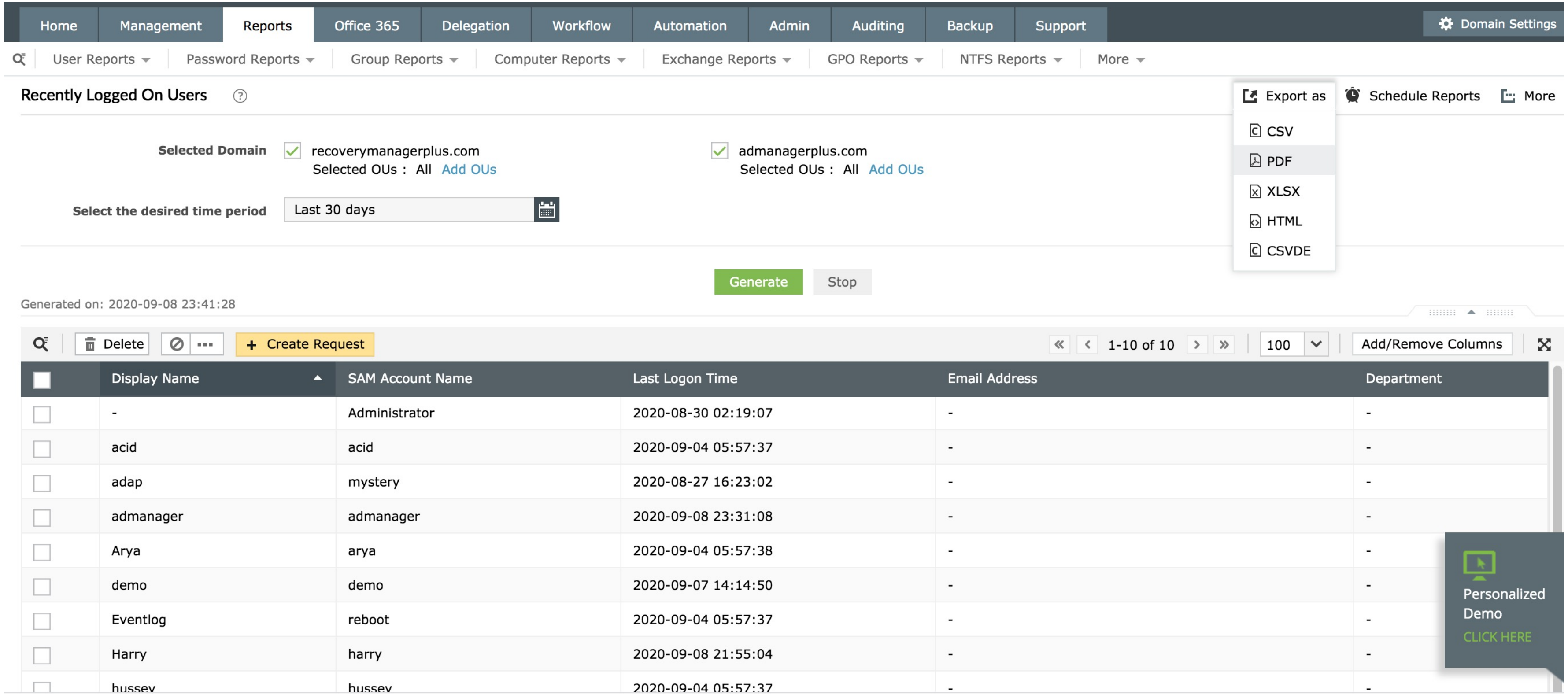
更改使用者的帳戶屬性

一覽視圖

啟用/禁用該帳戶 : 啟用

☐	全名	名	登錄名	帳戶逾期時間	帳戶狀態	最後登
☐	aaron es	aaron	aaronvanes@admanagerplus.com	永不過期	已啟用	0
☐	AbdulLatheef	Abdul	Laths@admanagerplus.com	永不過期	已啟用	0
☑	AldoOrnelas	Aldo	AOrnelas@admanagerplus.com	永不過期	已啟用	0
☐	Andres Valarezo	-	-	永不過期	已禁用	0
☐	asdfq	-	-	永不過期	已禁用	0
☐	BerndWinter	Bernd	BWinter@admanagerplus.com	永不過期	已啟用	0
☐	Billy Dee	Billy	billy.dee@admanagerplus.com	永不過期	已禁用	0
☐	Bobby Shew	Bobby	shewb@admanagerplus.com	永不過期	已啟用	0
☐	BrendaMayoral	-	-	永不過期	已禁用	0
☐	carlosj	Juan	carlosj@admanagerplus.com	永不過期	已禁用	0

AD綜合管理 – 即時報表 / 排程報表



Home
Management
Reports
Office 365
Delegation
Workflow
Automation
Admin
Auditing
Backup
Support
Domain Settings
User Reports
Password Reports
Group Reports
Computer Reports
Exchange Reports
GPO Reports
NTFS Reports
More
Export as
CSV
PDF
XLSX
HTML
CSVDE
Schedule Reports
More
Generate
Stop
Delete
Create Request
1-10 of 10
100
Add/Remove Columns
Personalized Demo
CLICK HERE

Recently Logged On Users

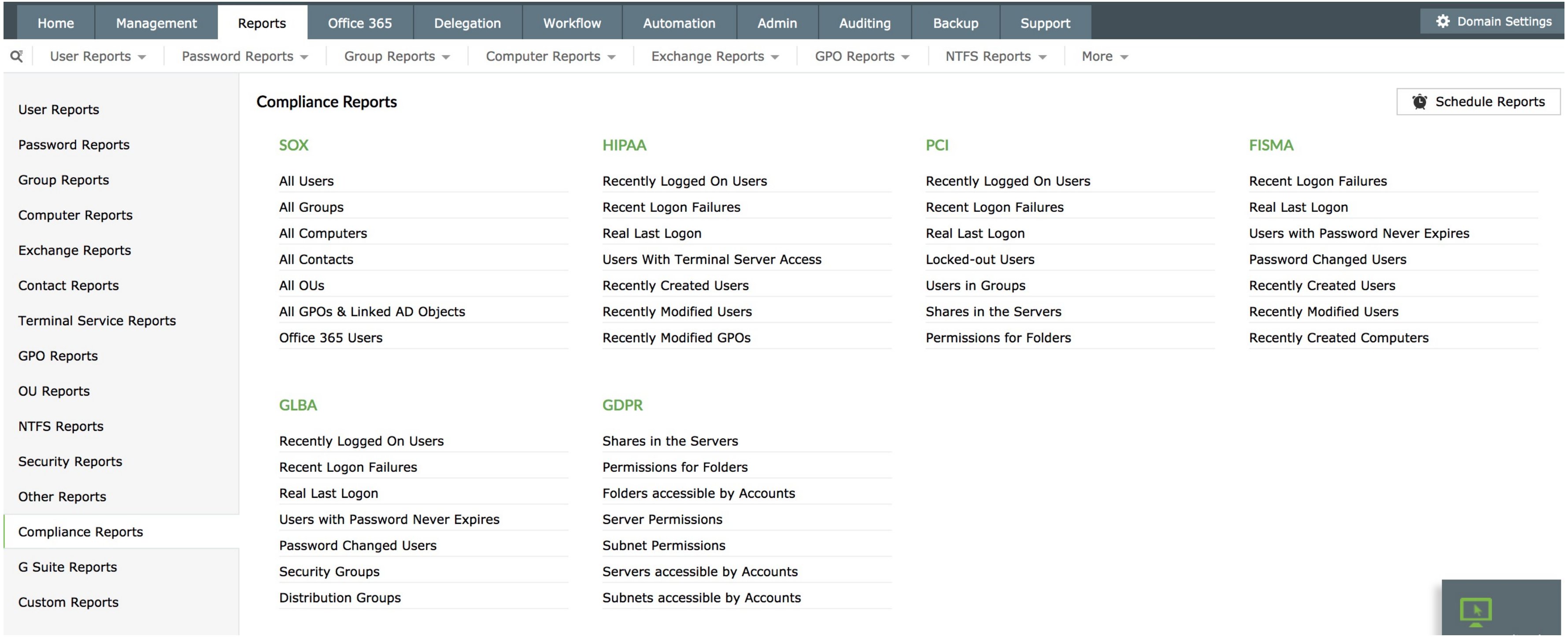
Selected Domain ☑ recoverymanagerplus.com
Selected OUs : All Add OUs
☑ admanagerplus.com
Selected OUs : All Add OUs

Select the desired time period Last 30 days

Generated on: 2020-09-08 23:41:28

☐	Display Name	SAM Account Name	Last Logon Time	Email Address	Department
☐	-	Administrator	2020-08-30 02:19:07	-	-
☐	acid	acid	2020-09-04 05:57:37	-	-
☐	adap	mystery	2020-08-27 16:23:02	-	-
☐	admanager	admanager	2020-09-08 23:31:08	-	-
☐	Arya	arya	2020-09-04 05:57:38	-	-
☐	demo	demo	2020-09-07 14:14:50	-	-
☐	Eventlog	reboot	2020-09-04 05:57:37	-	-
☐	Harry	harry	2020-09-08 21:55:04	-	-
☐	hussey	hussey	2020-09-04 05:57:37	-	-

AD綜合管理 – 稽核報表 / 自訂報表

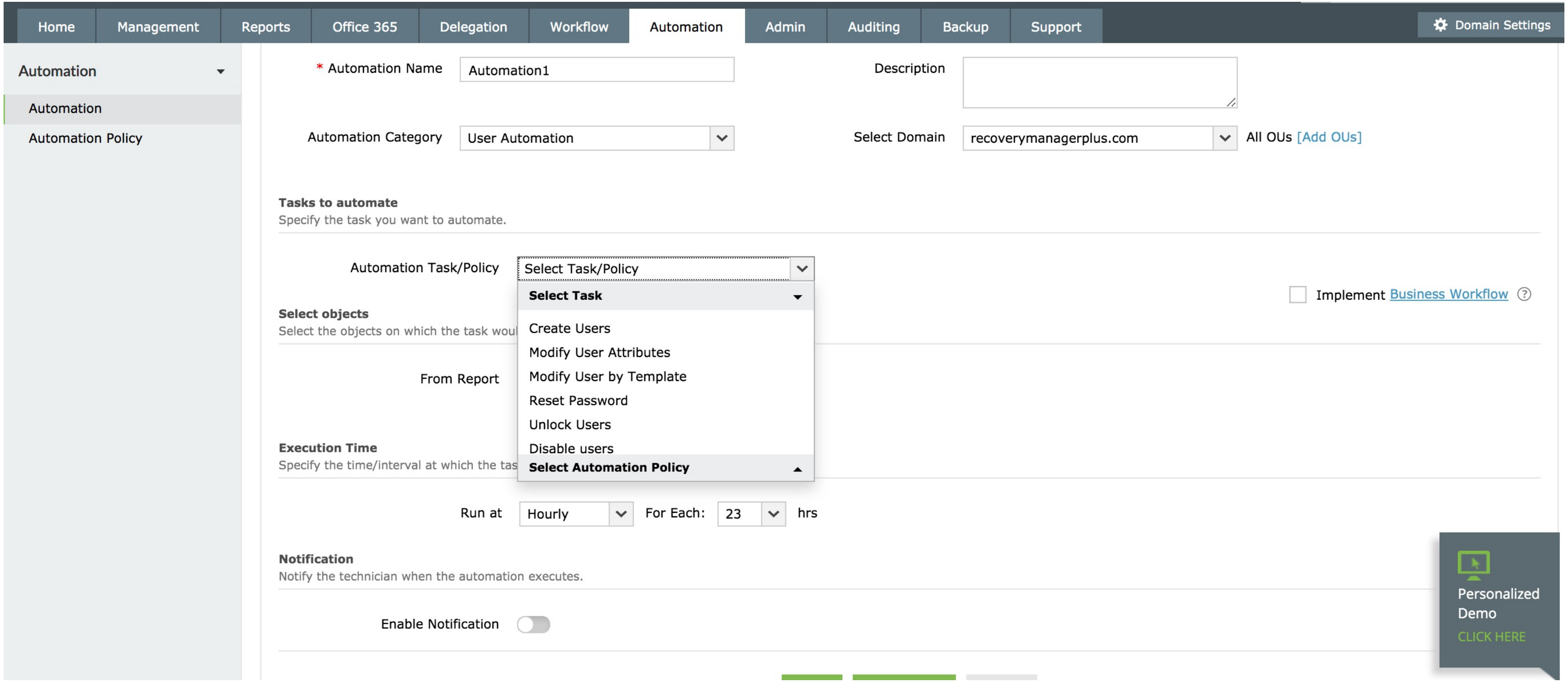

Home
Management
Reports
Office 365
Delegation
Workflow
Automation
Admin
Auditing
Backup
Support
Domain Settings
User Reports
Password Reports
Group Reports
Computer Reports
Exchange Reports
GPO Reports
NTFS Reports
More
User Reports
Password Reports
Group Reports
Computer Reports
Exchange Reports
Contact Reports
Terminal Service Reports
GPO Reports
OU Reports
NTFS Reports
Security Reports
Other Reports
Compliance Reports
G Suite Reports
Custom Reports
Schedule Reports

Compliance Reports

SOX	HIPAA	PCI	FISMA
All Users	Recently Logged On Users	Recently Logged On Users	Recent Logon Failures
All Groups	Recent Logon Failures	Recent Logon Failures	Real Last Logon
All Computers	Real Last Logon	Real Last Logon	Users with Password Never Expires
All Contacts	Users With Terminal Server Access	Locked-out Users	Password Changed Users
All OUs	Recently Created Users	Users in Groups	Recently Created Users
All GPOs & Linked AD Objects	Recently Modified Users	Shares in the Servers	Recently Modified Users
Office 365 Users	Recently Modified GPOs	Permissions for Folders	Recently Created Computers

GLBA	GDPR
Recently Logged On Users	Shares in the Servers
Recent Logon Failures	Permissions for Folders
Real Last Logon	Folders accessible by Accounts
Users with Password Never Expires	Server Permissions
Password Changed Users	Subnet Permissions
Security Groups	Servers accessible by Accounts
Distribution Groups	Subnets accessible by Accounts

AD綜合管理 – 無需Script的自動化任務或政策



Home
Management
Reports
Office 365
Delegation
Workflow
Automation
Admin
Auditing
Backup
Support
Domain Settings
Automation
Automation
Automation Policy

* Automation Name: Automation1

Description:

Automation Category: User Automation

Select Domain: recoverymanagerplus.com

All OUs [Add OUs]

Tasks to automate

Specify the task you want to automate.

Automation Task/Policy: Select Task/Policy

Select Task
Create Users
Modify User Attributes
Modify User by Template
Reset Password
Unlock Users
Disable users
Select Automation Policy

☐ Implement Business Workflow

Select objects

Select the objects on which the task woul

From Report

Execution Time

Specify the time/interval at which the tas

Run at: Hourly   For Each: 23 hrs

Notification

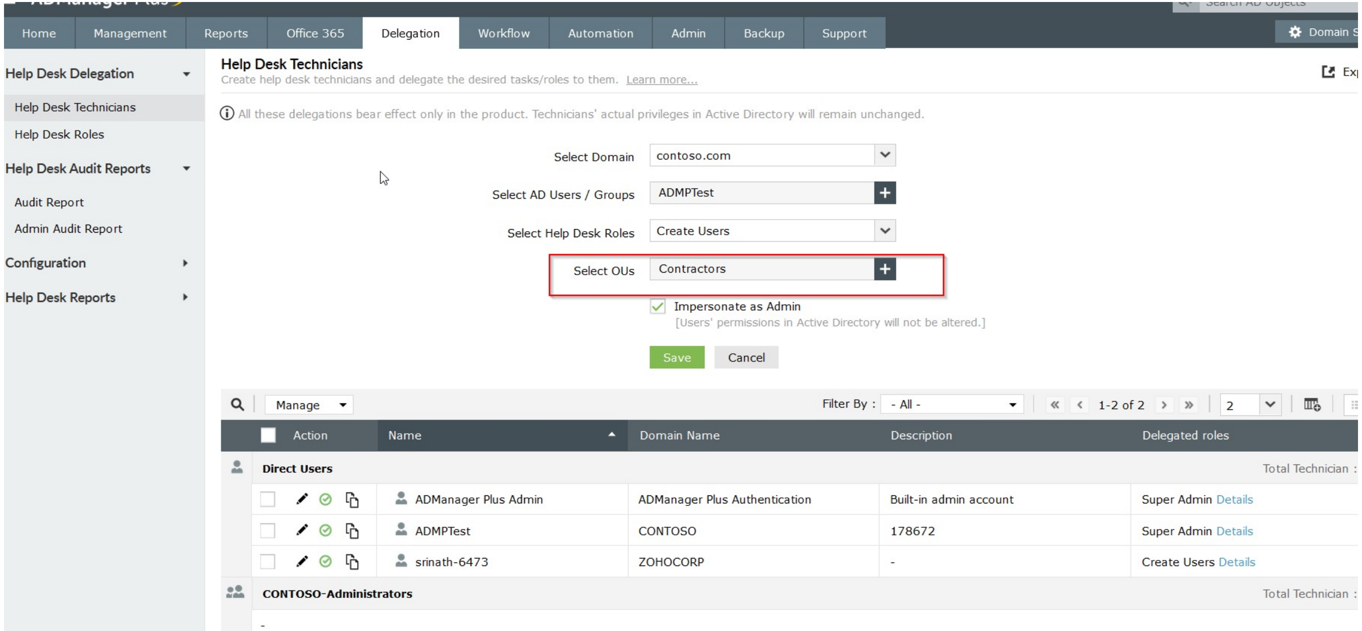
Notify the technician when the automation executes.

Enable Notification

Personalized Demo
CLICK HERE

使用情境 – 委任OU管理員

- 委任外點人員，當使用者遇到AD狀況時，提供即時協助


Home
Management
Reports
Office 365
Delegation
Workflow
Automation
Admin
Backup
Support
Domain S
Help Desk Delegation
Help Desk Technicians
Help Desk Roles
Help Desk Audit Reports
Audit Report
Admin Audit Report
Configuration
Help Desk Reports
Ex
Save
Cancel
Manage
Filter By :
- All -
1-2 of 2
2

Help Desk Technicians

Create help desk technicians and delegate the desired tasks/roles to them. Learn more...

ⓘ All these delegations bear effect only in the product. Technicians' actual privileges in Active Directory will remain unchanged.

Select Domain: contoso.com

Select AD Users / Groups: ADMPTest

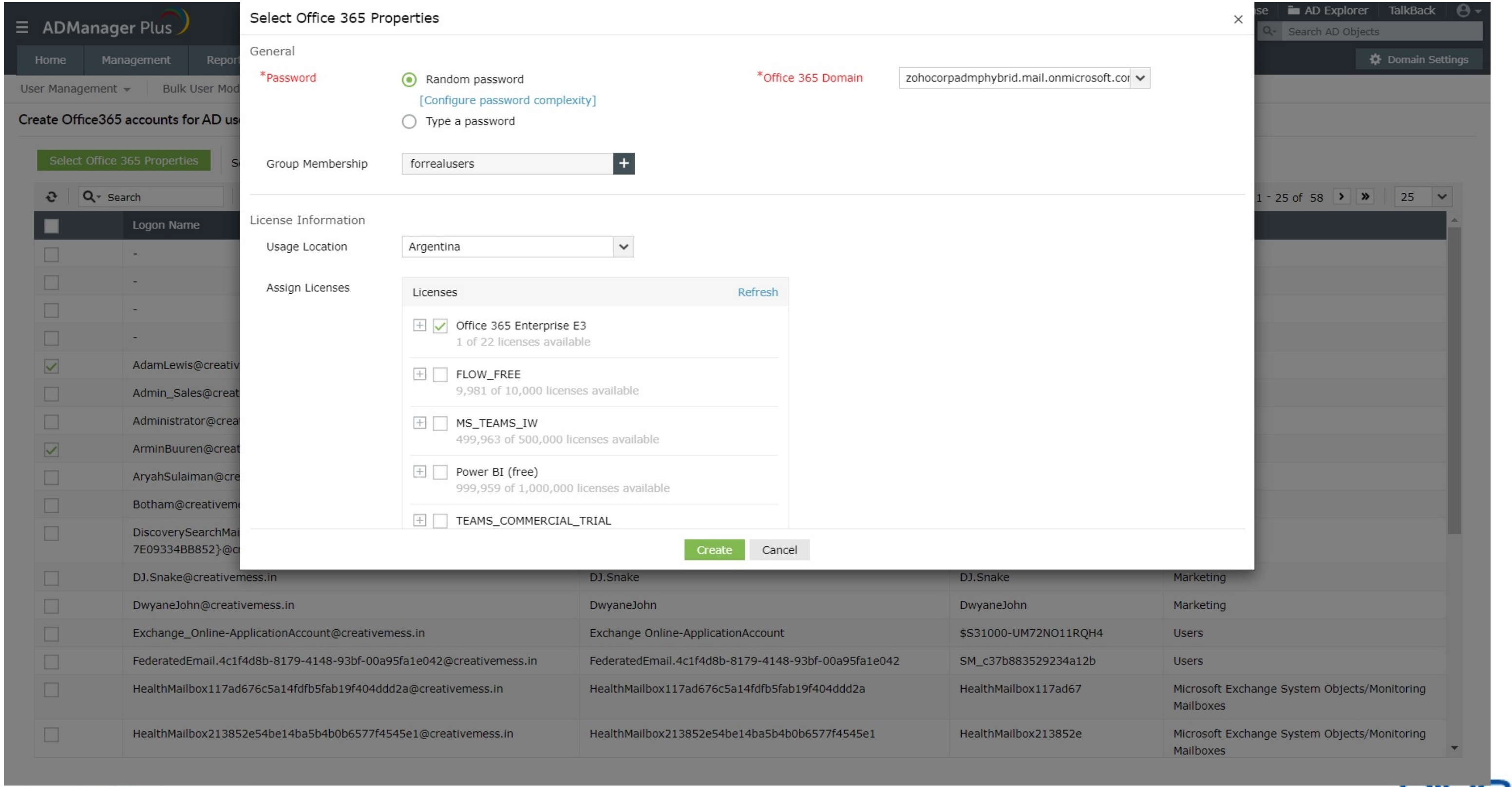
Select Help Desk Roles: Create Users

Select OUs: Contractors

☑ Impersonate as Admin
[Users' permissions in Active Directory will not be altered.]

Action	Name	Domain Name	Description	Delegated roles
Direct Users				Total Technician :
☐	ADManager Plus Admin	ADManager Plus Authentication	Built-in admin account	Super Admin Details
☐	ADMPTest	CONTOSO	178672	Super Admin Details
☐	srinath-6473	ZOHOCORP	-	Create Users Details
CONTOSO-Administrators				Total Technician :
-				

使用情境 – 套用O365帳號


ADManager Plus
Home
Management
Report
User Management
Bulk User Mod
Create Office365 accounts for AD us
Select Office 365 Properties
Search
Logon Name
AD Explorer
TalkBack
Search AD Objects
Domain Settings
1 - 25 of 58
25

Select Office 365 Properties

General

*Password: ● Random password [Configure password complexity] ○ Type a password

*Office 365 Domain: zohocorpadmphybrid.mail.onmicrosoft.com

Group Membership: forrealusers

License Information

Usage Location: Argentina

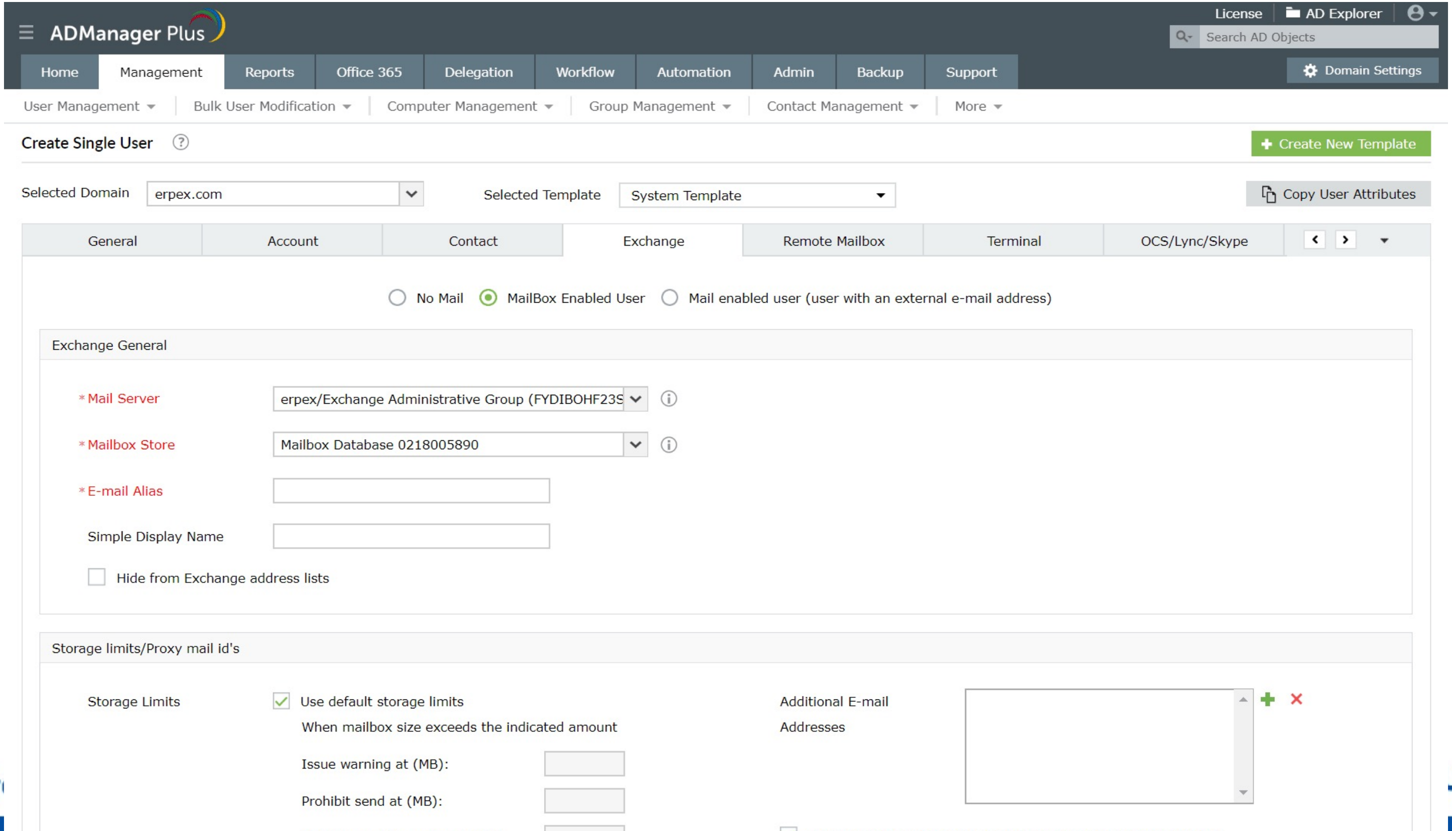
Assign Licenses:

Licenses
☑ Office 365 Enterprise E3 1 of 22 licenses available
☐ FLOW_FREE 9,981 of 10,000 licenses available
☐ MS_TEAMS_IW 499,963 of 500,000 licenses available
☐ Power BI (free) 999,959 of 1,000,000 licenses available
☐ TEAMS_COMMERCIAL_TRIAL

Refresh
Create
Cancel

DJ.Snake@creativemess.in	DJ.Snake	DJ.Snake	Marketing
DwyaneJohn@creativemess.in	DwyaneJohn	DwyaneJohn	Marketing
Exchange_Online-ApplicationAccount@creativemess.in	Exchange Online-ApplicationAccount	$S31000-UM72NO11RQH4	Users
FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042@creativemess.in	FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042	SM_c37b883529234a12b	Users
HealthMailbox117ad676c5a14fdfb5fab19f404ddd2a@creativemess.in	HealthMailbox117ad676c5a14fdfb5fab19f404ddd2a	HealthMailbox117ad67	Microsoft Exchange System Objects/Monitoring Mailboxes
HealthMailbox213852e54be14ba5b4b0b6577f4545e1@creativemess.in	HealthMailbox213852e54be14ba5b4b0b6577f4545e1	HealthMailbox213852e	Microsoft Exchange System Objects/Monitoring Mailboxes

使用情境 – 啟用Exchange帳號


ADManager Plus
License
AD Explorer
Search AD Objects
Home
Management
Reports
Office 365
Delegation
Workflow
Automation
Admin
Backup
Support
Domain Settings
User Management
Bulk User Modification
Computer Management
Group Management
Contact Management
More
Create New Template
Copy User Attributes
General
Account
Contact
Exchange
Remote Mailbox
Terminal
OCS/Lync/Skype

Create Single User

Selected Domain: erpex.com

Selected Template: System Template

○ No Mail ● MailBox Enabled User ○ Mail enabled user (user with an external e-mail address)

Exchange General

* Mail Server: erpex/Exchange Administrative Group (FYDIBOHF23S

* Mailbox Store: Mailbox Database 0218005890

* E-mail Alias:

Simple Display Name:

☐ Hide from Exchange address lists

Storage limits/Proxy mail id's

Storage Limits: ☑ Use default storage limits

When mailbox size exceeds the indicated amount

Issue warning at (MB):

Prohibit send at (MB):

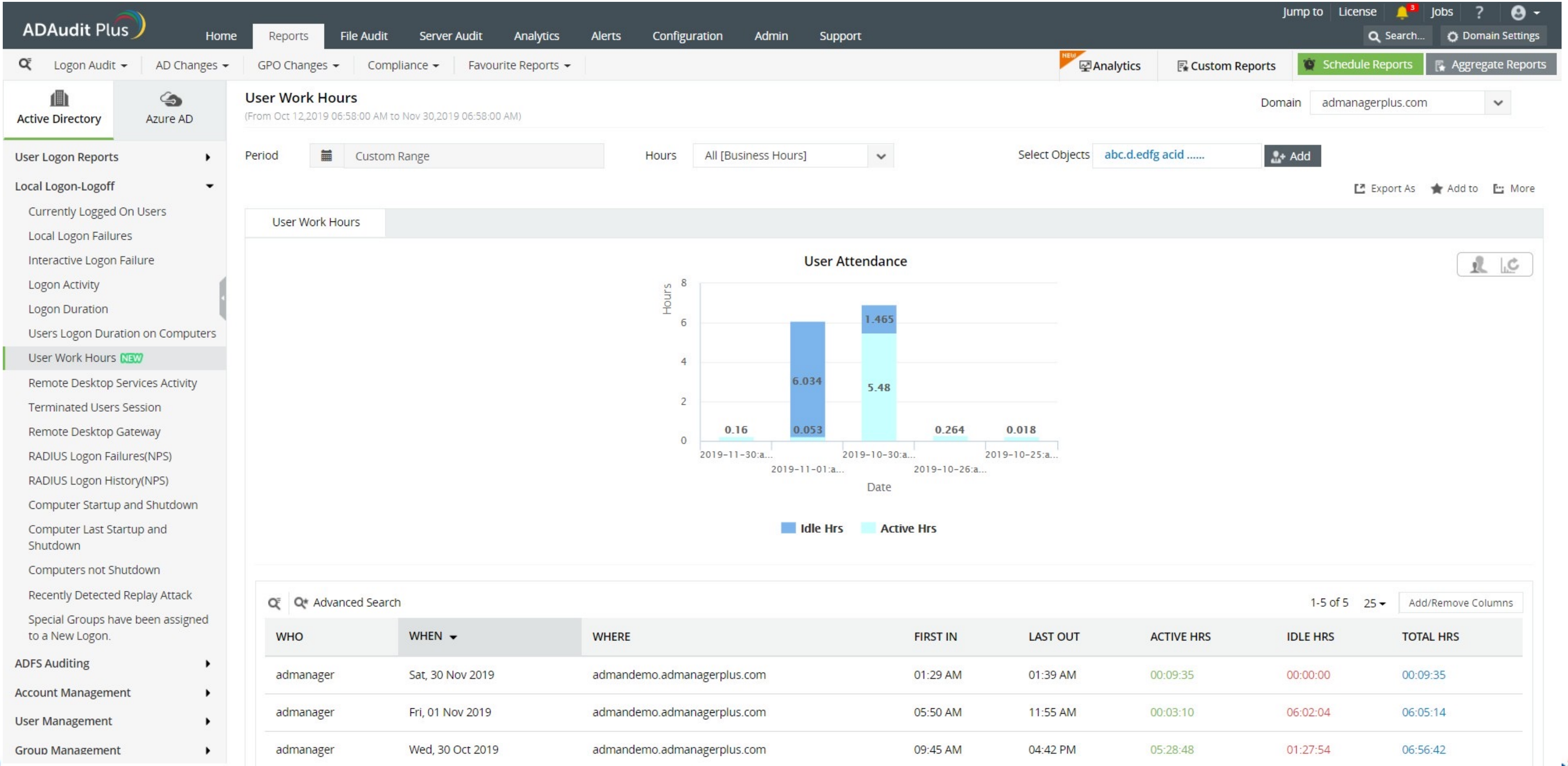
Additional E-mail Addresses

AD稽核

AD稽核 – 稽核面向

- Active Directory
- 檔案伺服器
- 群組原則變更
- Windows 伺服器
- Workstation
- 使用者行為分析
- 特權帳號監控

AD稽核 – 使用者上線時間報表


ADAudit Plus
Home
Reports
File Audit
Server Audit
Analytics
Alerts
Configuration
Admin
Support
Jump to
License
Jobs
?
Search...
Domain Settings
Logon Audit
AD Changes
GPO Changes
Compliance
Favourite Reports
Analytics
Custom Reports
Schedule Reports
Aggregate Reports
Active Directory
Azure AD
User Logon Reports
Local Logon-Logoff
Currently Logged On Users
Local Logon Failures
Interactive Logon Failure
Logon Activity
Logon Duration
Users Logon Duration on Computers
User Work Hours NEW
Remote Desktop Services Activity
Terminated Users Session
Remote Desktop Gateway
RADIUS Logon Failures(NPS)
RADIUS Logon History(NPS)
Computer Startup and Shutdown
Computer Last Startup and Shutdown
Computers not Shutdown
Recently Detected Replay Attack
Special Groups have been assigned to a New Logon.
ADFS Auditing
Account Management
User Management
Group Management
Add
Export As
Add to
More
User Attendance
Hours
8
6
4
2
0
1.465
6.034
5.48
0.16
0.053
0.264
0.018
2019-11-30:a...
2019-11-01:a...
2019-10-30:a...
2019-10-26:a...
2019-10-25:a...
Date
Idle Hrs
Active Hrs
Advanced Search
25
Add/Remove Columns

User Work Hours

(From Oct 12,2019 06:58:00 AM to Nov 30,2019 06:58:00 AM)

Domain: admanagerplus.com

Period: Custom Range

Hours: All [Business Hours]

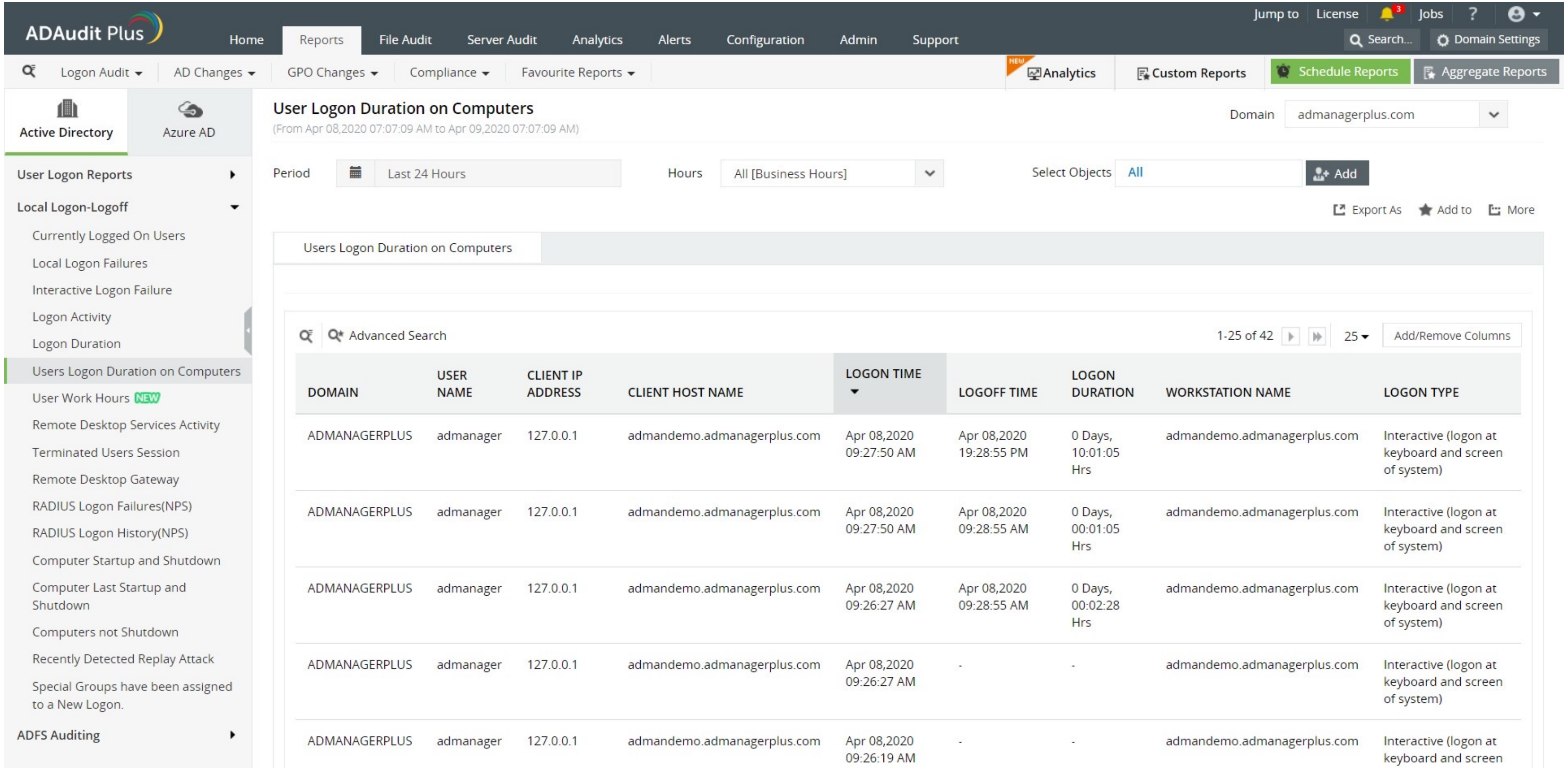
Select Objects: abc.d.edfg acid ......

User Work Hours

1-5 of 5

WHO	WHEN	WHERE	FIRST IN	LAST OUT	ACTIVE HRS	IDLE HRS	TOTAL HRS
admanager	Sat, 30 Nov 2019	admandemo.admanagerplus.com	01:29 AM	01:39 AM	00:09:35	00:00:00	00:09:35
admanager	Fri, 01 Nov 2019	admandemo.admanagerplus.com	05:50 AM	11:55 AM	00:03:10	06:02:04	06:05:14
admanager	Wed, 30 Oct 2019	admandemo.admanagerplus.com	09:45 AM	04:42 PM	05:28:48	01:27:54	06:56:42

AD稽核 – 使用者登入操作軌跡


ADAudit Plus
Home
Reports
File Audit
Server Audit
Analytics
Alerts
Configuration
Admin
Support
Jump to
License
Jobs
?
Search...
Domain Settings
Logon Audit
AD Changes
GPO Changes
Compliance
Favourite Reports
NEW
Analytics
Custom Reports
Schedule Reports
Aggregate Reports
Active Directory
Azure AD
User Logon Reports
Local Logon-Logoff
Currently Logged On Users
Local Logon Failures
Interactive Logon Failure
Logon Activity
Logon Duration
Users Logon Duration on Computers
User Work Hours NEW
Remote Desktop Services Activity
Terminated Users Session
Remote Desktop Gateway
RADIUS Logon Failures(NPS)
RADIUS Logon History(NPS)
Computer Startup and Shutdown
Computer Last Startup and Shutdown
Computers not Shutdown
Recently Detected Replay Attack
Special Groups have been assigned to a New Logon.
ADFS Auditing
Add
Export As
Add to
More
Users Logon Duration on Computers
Advanced Search
1-25 of 42
25
Add/Remove Columns

User Logon Duration on Computers

(From Apr 08,2020 07:07:09 AM to Apr 09,2020 07:07:09 AM)

Domain: admanagerplus.com

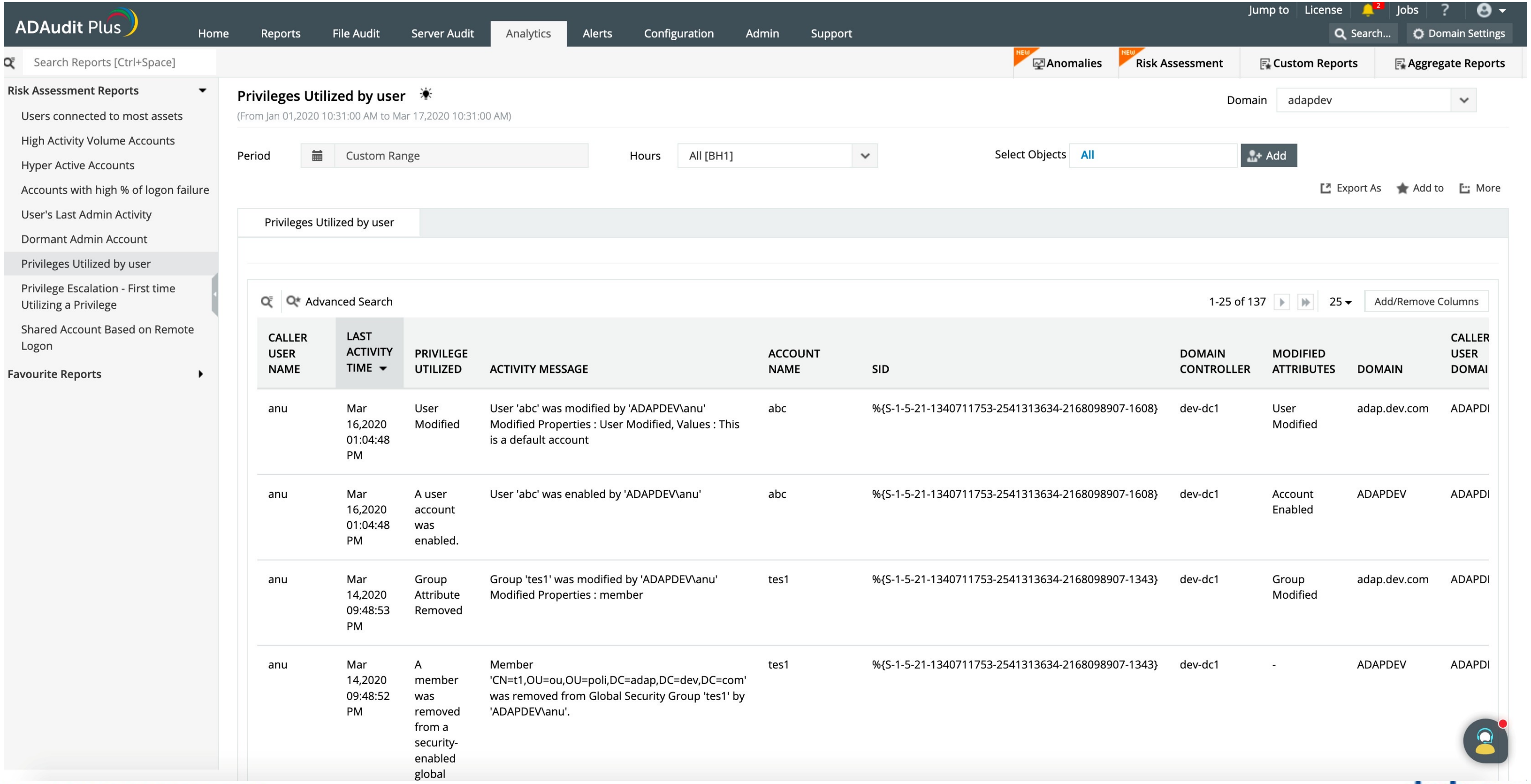
Period: Last 24 Hours

Hours: All [Business Hours]

Select Objects: All

DOMAIN	USER NAME	CLIENT IP ADDRESS	CLIENT HOST NAME	LOGON TIME	LOGOFF TIME	LOGON DURATION	WORKSTATION NAME	LOGON TYPE
ADMANAGERPLUS	admanager	127.0.0.1	admandemo.admanagerplus.com	Apr 08,2020 09:27:50 AM	Apr 08,2020 19:28:55 PM	0 Days, 10:01:05 Hrs	admandemo.admanagerplus.com	Interactive (logon at keyboard and screen of system)
ADMANAGERPLUS	admanager	127.0.0.1	admandemo.admanagerplus.com	Apr 08,2020 09:27:50 AM	Apr 08,2020 09:28:55 AM	0 Days, 00:01:05 Hrs	admandemo.admanagerplus.com	Interactive (logon at keyboard and screen of system)
ADMANAGERPLUS	admanager	127.0.0.1	admandemo.admanagerplus.com	Apr 08,2020 09:26:27 AM	Apr 08,2020 09:28:55 AM	0 Days, 00:02:28 Hrs	admandemo.admanagerplus.com	Interactive (logon at keyboard and screen of system)
ADMANAGERPLUS	admanager	127.0.0.1	admandemo.admanagerplus.com	Apr 08,2020 09:26:27 AM	-	-	admandemo.admanagerplus.com	Interactive (logon at keyboard and screen of system)
ADMANAGERPLUS	admanager	127.0.0.1	admandemo.admanagerplus.com	Apr 08,2020 09:26:19 AM	-	-	admandemo.admanagerplus.com	Interactive (logon at keyboard and screen

AD稽核 – 異常登入資安事件報表


ADAudit Plus
Home
Reports
File Audit
Server Audit
Analytics
Alerts
Configuration
Admin
Support
Jump to
License
Jobs
?
Search...
Domain Settings
Search Reports [Ctrl+Space]
Anomalies
Risk Assessment
Custom Reports
Aggregate Reports
Risk Assessment Reports
Users connected to most assets
High Activity Volume Accounts
Hyper Active Accounts
Accounts with high % of logon failure
User's Last Admin Activity
Dormant Admin Account
Privileges Utilized by user
Privilege Escalation - First time Utilizing a Privilege
Shared Account Based on Remote Logon
Favourite Reports
Add
Export As
Add to
More
Privileges Utilized by user
Advanced Search
1-25 of 137
25
Add/Remove Columns

Privileges Utilized by user

(From Jan 01,2020 10:31:00 AM to Mar 17,2020 10:31:00 AM)

Domain: adapdev

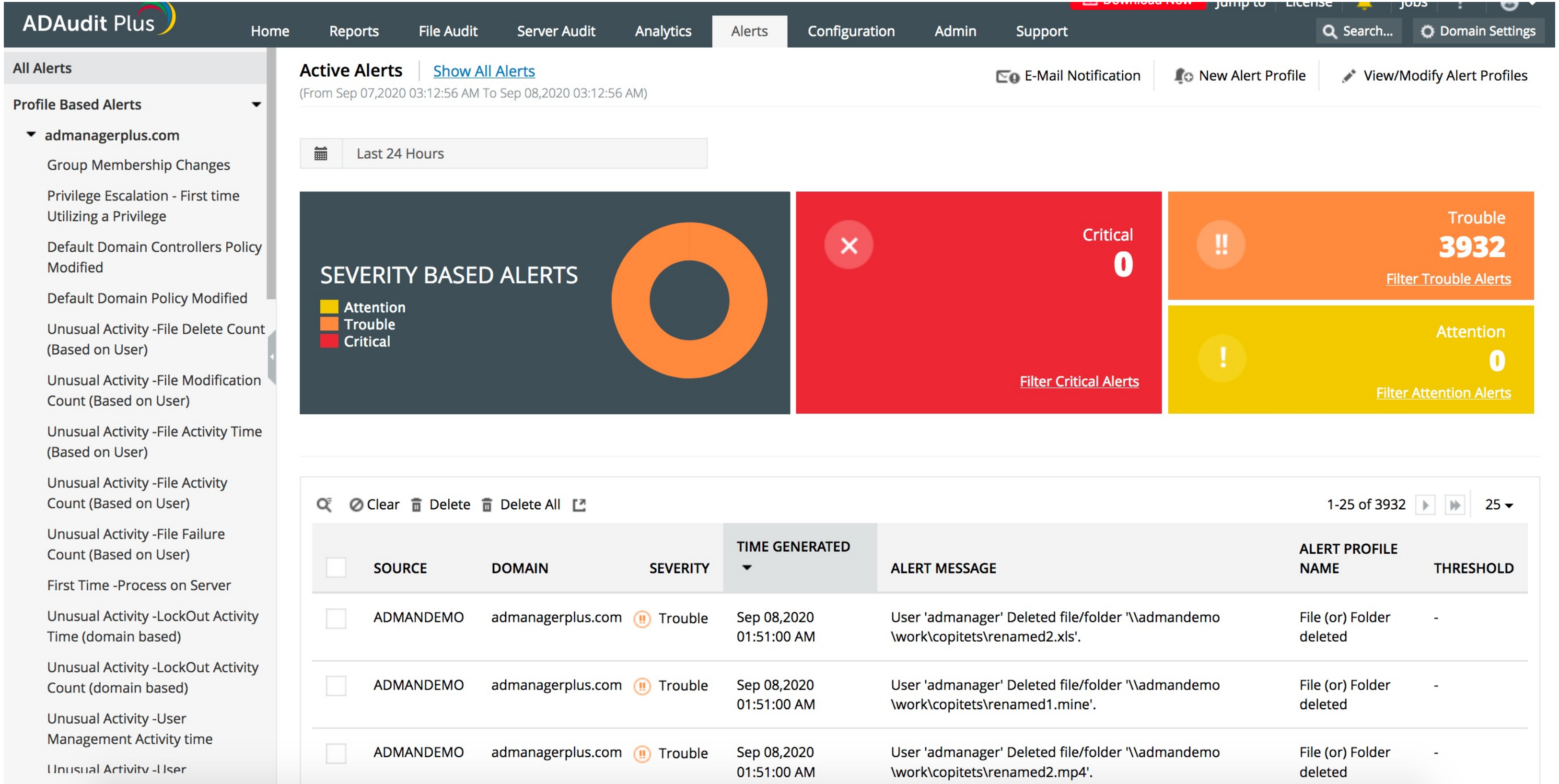
Period: Custom Range

Hours: All [BH1]

Select Objects: All

CALLER USER NAME	LAST ACTIVITY TIME	PRIVILEGE UTILIZED	ACTIVITY MESSAGE	ACCOUNT NAME	SID	DOMAIN CONTROLLER	MODIFIED ATTRIBUTES	DOMAIN	CALLER USER DOMAI
anu	Mar 16,2020 01:04:48 PM	User Modified	User 'abc' was modified by 'ADAPDEV\anu' Modified Properties : User Modified, Values : This is a default account	abc	%{S-1-5-21-1340711753-2541313634-2168098907-1608}	dev-dc1	User Modified	adap.dev.com	ADAPDI
anu	Mar 16,2020 01:04:48 PM	A user account was enabled.	User 'abc' was enabled by 'ADAPDEV\anu'	abc	%{S-1-5-21-1340711753-2541313634-2168098907-1608}	dev-dc1	Account Enabled	ADAPDEV	ADAPDI
anu	Mar 14,2020 09:48:53 PM	Group Attribute Removed	Group 'tes1' was modified by 'ADAPDEV\anu' Modified Properties : member	tes1	%{S-1-5-21-1340711753-2541313634-2168098907-1343}	dev-dc1	Group Modified	adap.dev.com	ADAPDI
anu	Mar 14,2020 09:48:52 PM	A member was removed from a security-enabled global	Member 'CN=t1,OU=ou,OU=poli,DC=adap,DC=dev,DC=com' was removed from Global Security Group 'tes1' by 'ADAPDEV\anu'.	tes1	%{S-1-5-21-1340711753-2541313634-2168098907-1343}	dev-dc1	-	ADAPDEV	ADAPDI

AD稽核 – 即時告警機制 / 自動執行Script


ADAudit Plus
Home
Reports
File Audit
Server Audit
Analytics
Alerts
Configuration
Admin
Support
Search...
Domain Settings
All Alerts
Profile Based Alerts
admanagerplus.com
Group Membership Changes
Privilege Escalation - First time Utilizing a Privilege
Default Domain Controllers Policy Modified
Default Domain Policy Modified
Unusual Activity -File Delete Count (Based on User)
Unusual Activity -File Modification Count (Based on User)
Unusual Activity -File Activity Time (Based on User)
Unusual Activity -File Activity Count (Based on User)
Unusual Activity -File Failure Count (Based on User)
First Time -Process on Server
Unusual Activity -LockOut Activity Time (domain based)
Unusual Activity -LockOut Activity Count (domain based)
Unusual Activity -User Management Activity time
Unusual Activity -User
E-Mail Notification
New Alert Profile
View/Modify Alert Profiles
Clear
Delete
Delete All
25

Active Alerts Show All Alerts

(From Sep 07,2020 03:12:56 AM To Sep 08,2020 03:12:56 AM)

Last 24 Hours

SEVERITY BASED ALERTS

- 🟨 Attention
- 🟧 Trouble
- 🟥 Critical

Critical 0 Filter Critical Alerts

Trouble 3932 Filter Trouble Alerts

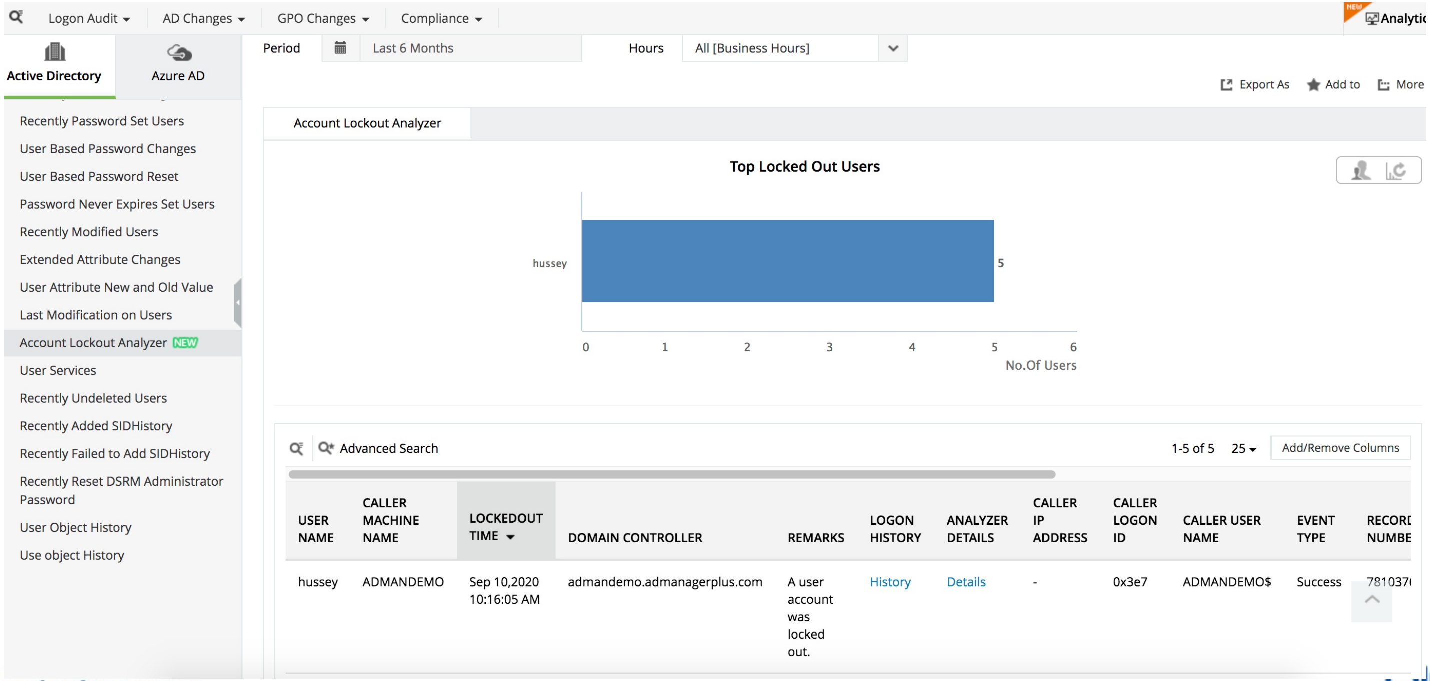
Attention 0 Filter Attention Alerts

1-25 of 3932

☐	SOURCE	DOMAIN	SEVERITY	TIME GENERATED	ALERT MESSAGE	ALERT PROFILE NAME	THRESHOLD
☐	ADMANDEMO	admanagerplus.com	Trouble	Sep 08,2020 01:51:00 AM	User 'admanager' Deleted file/folder '\\admandemo \work\copitets\renamed2.xls'.	File (or) Folder deleted	-
☐	ADMANDEMO	admanagerplus.com	Trouble	Sep 08,2020 01:51:00 AM	User 'admanager' Deleted file/folder '\\admandemo \work\copitets\renamed1.mine'.	File (or) Folder deleted	-
☐	ADMANDEMO	admanagerplus.com	Trouble	Sep 08,2020 01:51:00 AM	User 'admanager' Deleted file/folder '\\admandemo \work\copitets\renamed2.mp4'.	File (or) Folder deleted	-

使用情境 – 最常被暴力破解的帳號

- 常常被鎖住的帳號，往往都是惡意存取的目標


Logon Audit
AD Changes
GPO Changes
Compliance
Analytic
Active Directory
Azure AD
Recently Password Set Users
User Based Password Changes
User Based Password Reset
Password Never Expires Set Users
Recently Modified Users
Extended Attribute Changes
User Attribute New and Old Value
Last Modification on Users
Account Lockout Analyzer NEW
User Services
Recently Undeleted Users
Recently Added SIDHistory
Recently Failed to Add SIDHistory
Recently Reset DSRM Administrator Password
User Object History
Use object History
Export As
Add to
More
Account Lockout Analyzer
Top Locked Out Users
hussey
5
0
1
2
3
4
5
6
No.Of Users
Advanced Search
1-5 of 5
25
Add/Remove Columns

Period: Last 6 Months

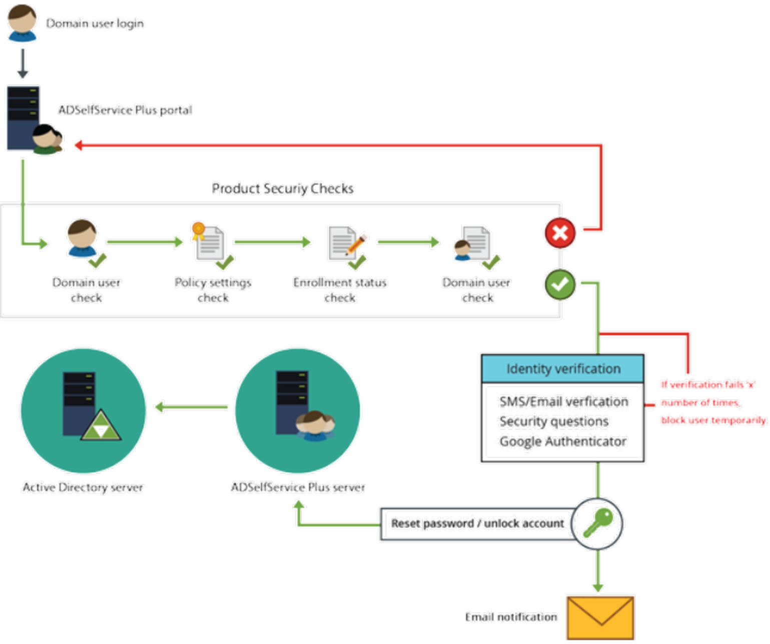
Hours: All [Business Hours]

USER NAME	CALLER MACHINE NAME	LOCKEDOUT TIME	DOMAIN CONTROLLER	REMARKS	LOGON HISTORY	ANALYZER DETAILS	CALLER IP ADDRESS	CALLER LOGON ID	CALLER USER NAME	EVENT TYPE	RECOR NUMBE
hussey	ADMANDEMO	Sep 10,2020 10:16:05 AM	admandemo.admanagerplus.com	A user account was locked out.	History	Details	-	0x3e7	ADMANDEMO$	Success	781037

AD自主管理

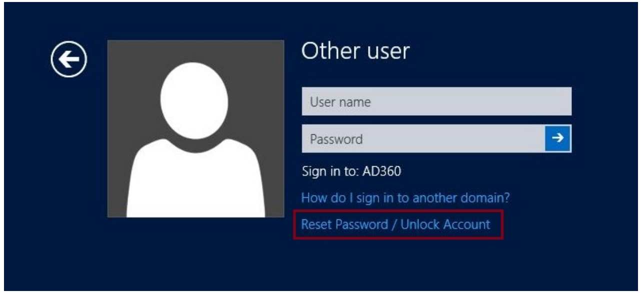
AD自主管理 – 用戶自主管理密碼與解鎖

- 四階段安全驗證，確保真實用戶
- 多因素驗證，確保正確用戶
- 管理員能即時收到使用者密碼修改/使用者帳戶解鎖事件



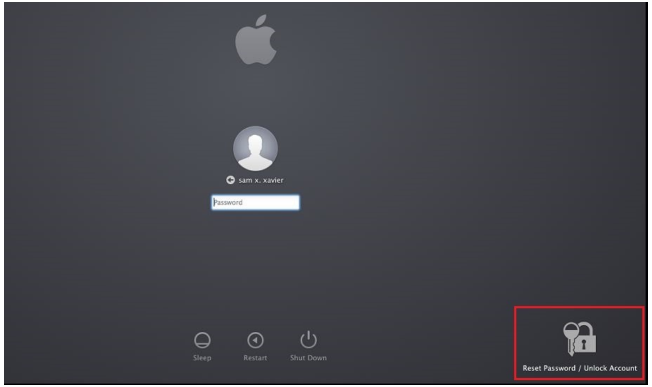
Domain user login
ADSelfService Plus portal
Product Securiy Checks
Domain user check
Policy settings check
Enrollment status check
Domain user check
Identity verification
SMS/Email verfication
Security questions
Google Authenticator
If verification fails 'x' number of times, block user temporarily.
Active Directory server
ADSelfService Plus server
Reset password / unlock account
Email notification

AD自主管理 – 整合各平台登入介面

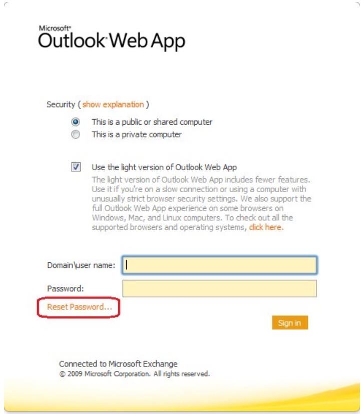

Other user
User name
Password
How do I sign in to another domain?
Reset Password / Unlock Account

Sign in to: AD360

Windows


sam x. xavier
Password
Sleep
Restart
Shut Down
Reset Password / Unlock Account

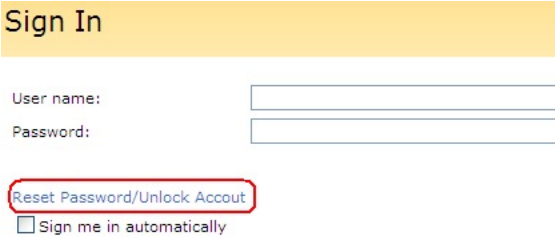
MacOS


Microsoft Outlook Web App
Security (show explanation)
● This is a public or shared computer
○ This is a private computer
☑ Use the light version of Outlook Web App
Domain\user name:
Password:
Reset Password...
Sign in

The light version of Outlook Web App includes fewer features. Use it if you're on a slow connection or using a computer with unusually strict browser security settings. We also support the full Outlook Web App experience on some browsers on Windows, Mac, and Linux computers. To check out all the supported browsers and operating systems, click here.

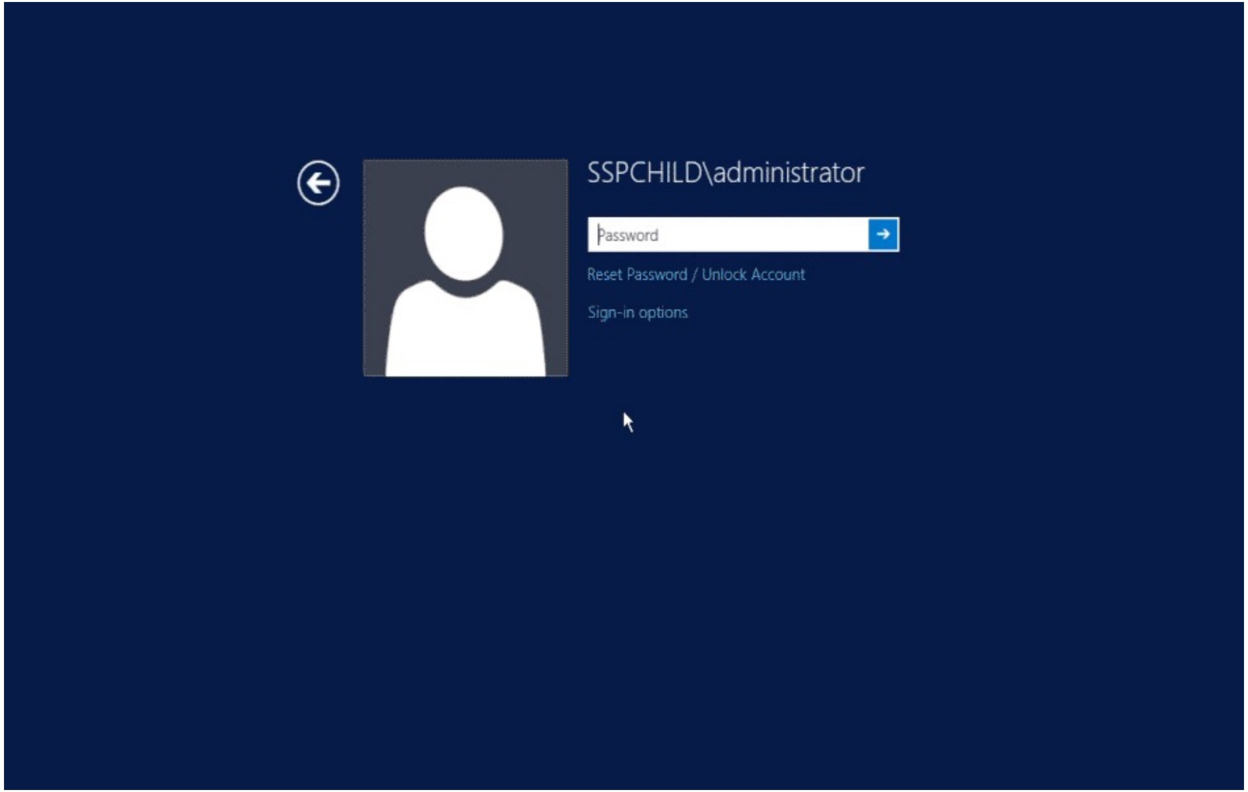
Connected to Microsoft Exchange
© 2009 Microsoft Corporation. All rights reserved.

O365


Sign In
User name:
Password:
Reset Password/Unlock Accout
☐ Sign me in automatically

SharePoint

AD自主管理 – 登入多一層保護

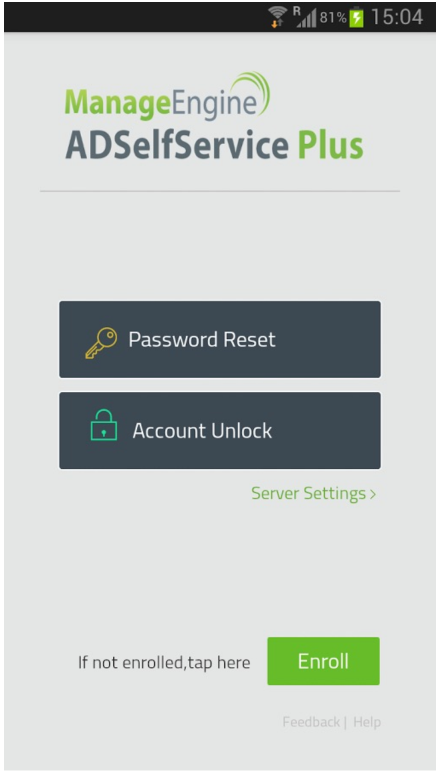


SSPCHILD\administrator

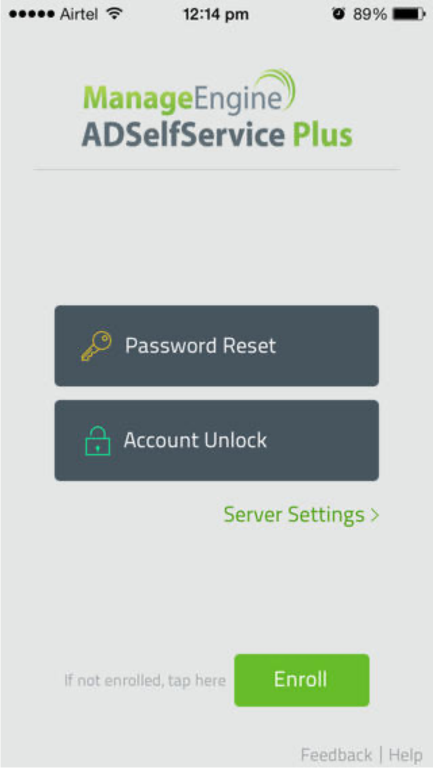
Password
Reset Password / Unlock Account
Sign-in options

AD自主管理 – 支援行動裝置App

- 隨時重置密碼與解鎖
- 推播重要訊息
- 管理者也可以透過App審核驗證用戶

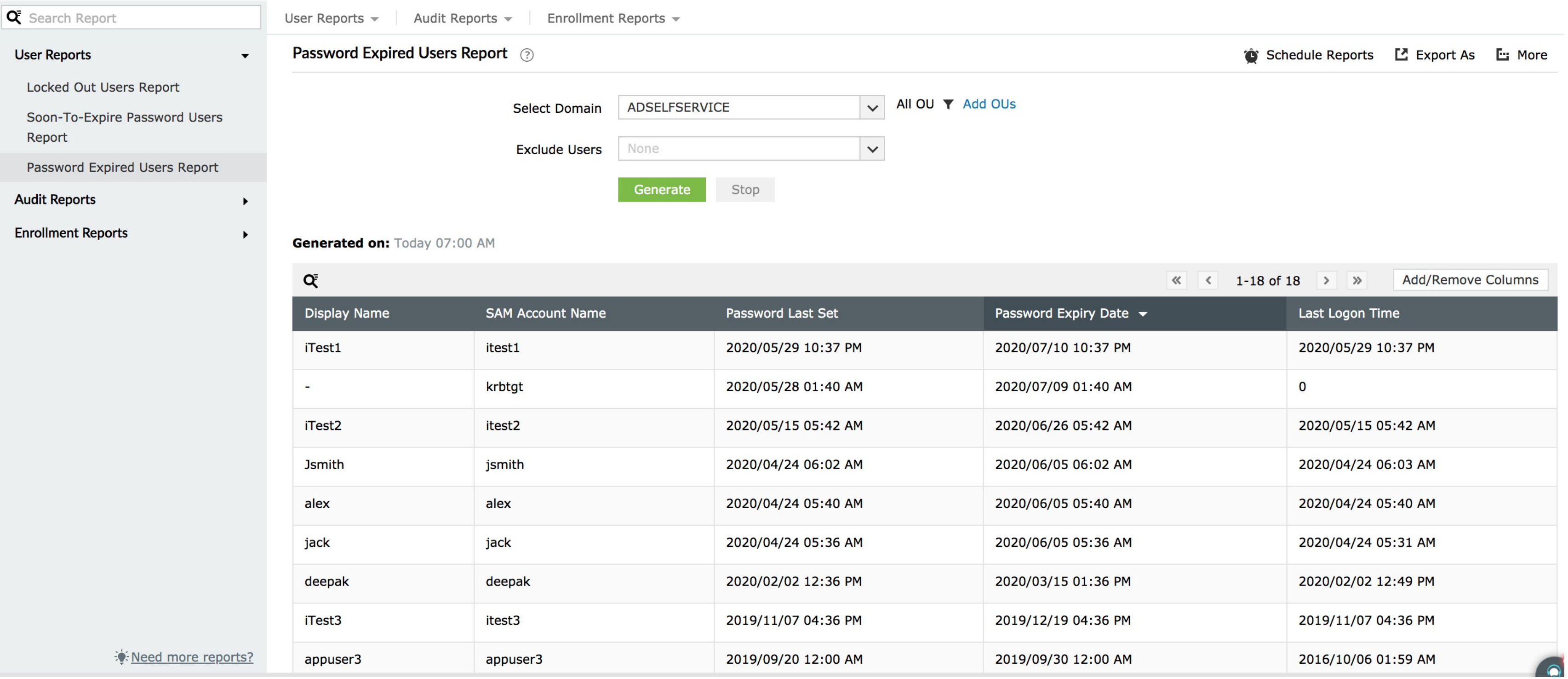

81% 15:04
ManageEngine
ADSelfService Plus
Password Reset
Account Unlock
Server Settings ›
If not enrolled,tap here
Enroll
Feedback | Help

Android


●●●●● Airtel 12:14 pm 89%
ManageEngine
ADSelfService Plus
Password Reset
Account Unlock
Server Settings ›
If not enrolled, tap here
Enroll
Feedback | Help

iOS

AD自主管理 – 身份驗證相關報表


Search Report
User Reports
Audit Reports
Enrollment Reports
User Reports
Locked Out Users Report
Soon-To-Expire Password Users Report
Password Expired Users Report
Audit Reports
Enrollment Reports
Need more reports?
Schedule Reports
Export As
More
Generate
Stop
Add OUs
1-18 of 18
Add/Remove Columns

Password Expired Users Report

Select Domain: ADSELFSERVICE

All OU

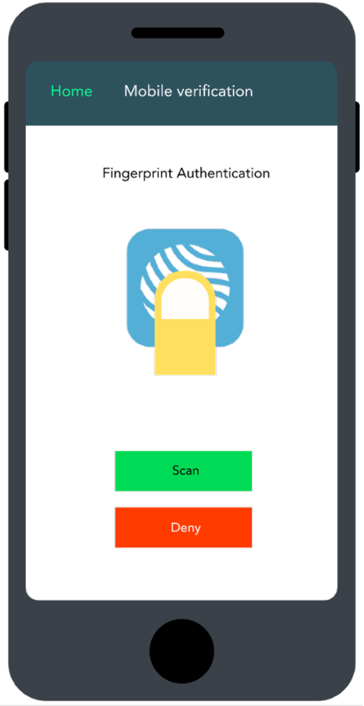
Exclude Users: None

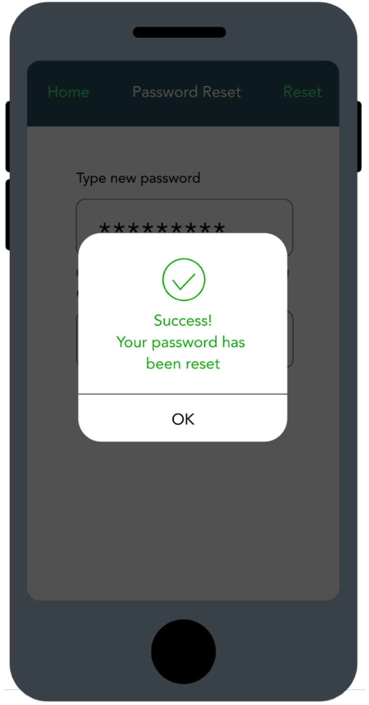
Generated on: Today 07:00 AM

Display Name	SAM Account Name	Password Last Set	Password Expiry Date	Last Logon Time
iTest1	itest1	2020/05/29 10:37 PM	2020/07/10 10:37 PM	2020/05/29 10:37 PM
-	krbtgt	2020/05/28 01:40 AM	2020/07/09 01:40 AM	0
iTest2	itest2	2020/05/15 05:42 AM	2020/06/26 05:42 AM	2020/05/15 05:42 AM
Jsmith	jsmith	2020/04/24 06:02 AM	2020/06/05 06:02 AM	2020/04/24 06:03 AM
alex	alex	2020/04/24 05:40 AM	2020/06/05 05:40 AM	2020/04/24 05:40 AM
jack	jack	2020/04/24 05:36 AM	2020/06/05 05:36 AM	2020/04/24 05:31 AM
deepak	deepak	2020/02/02 12:36 PM	2020/03/15 01:36 PM	2020/02/02 12:49 PM
iTest3	itest3	2019/11/07 04:36 PM	2019/12/19 04:36 PM	2019/11/07 04:36 PM
appuser3	appuser3	2019/09/20 12:00 AM	2019/09/30 12:00 AM	2016/10/06 01:59 AM

使用情境 – 當外點人員常需要管理員解鎖

- 讓外點人員自主管理。
- 節省外點人員等待時間。
- 讓管理員有更多時間，處理資安事件。


Home
Mobile verification
Fingerprint Authentication
Scan
Deny


Home
Password Reset
Reset
OK

Type new password

****

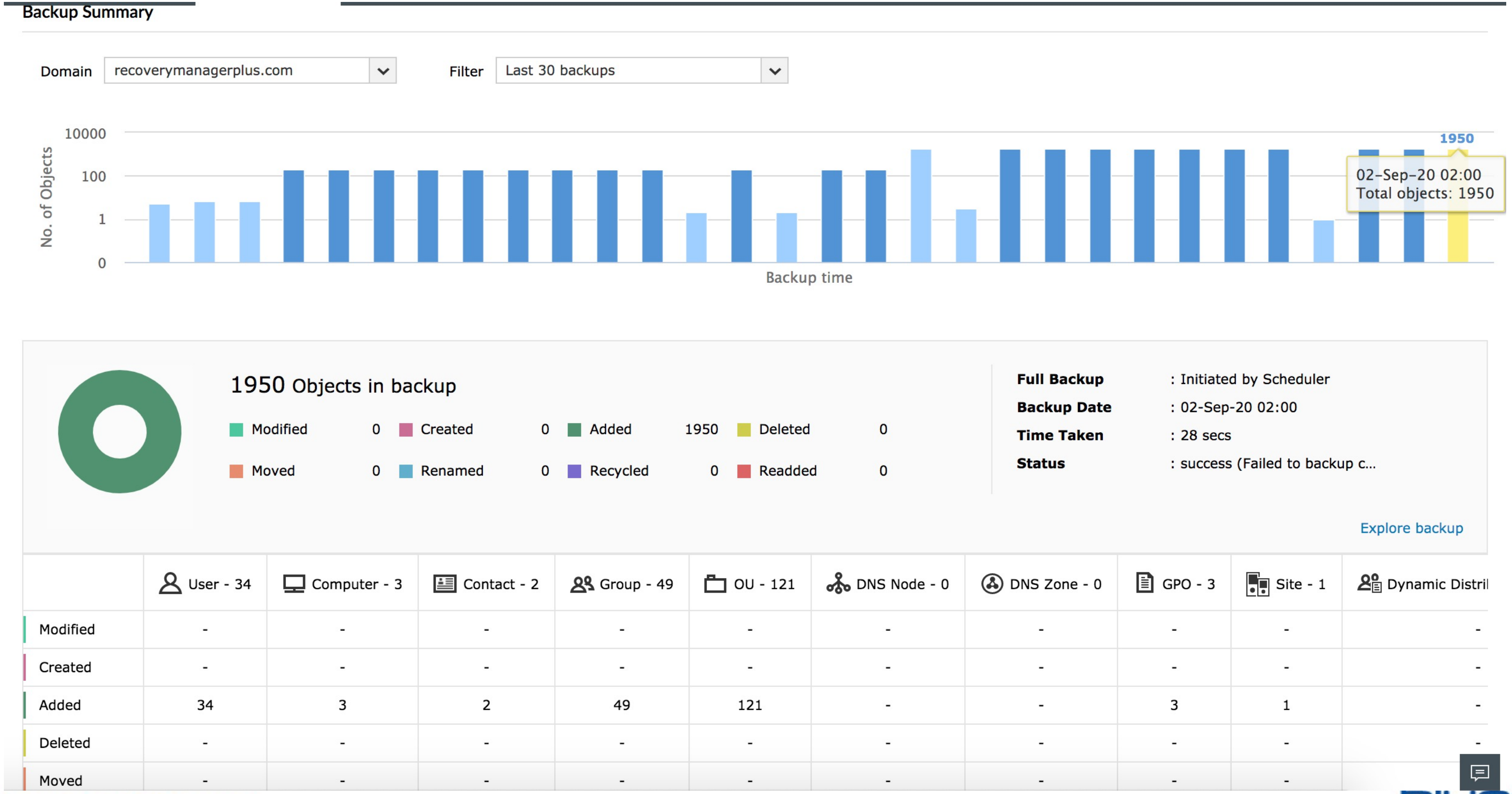
Success!
Your password has
been reset

AD備份還原

AD備份還原 – 無需直接觸碰網域控制器

- 備份還原AD物件，包含：
  - 使用者
  - 電腦
  - 聯絡資訊
  - 群組
  - OU
  - GPO
  - DNS
- 比較前後差異，也可復原，最小化錯誤

AD備份還原 – 支援增量備份



Backup Summary

Domain: recoverymanagerplus.com

Filter: Last 30 backups

02-Sep-20 02:00
Total objects: 1950

1950 Objects in backup

🟩 Modified	0	🟥 Created	0	🟩 Added	1950	🟨 Deleted	0
🟧 Moved	0	🟦 Renamed	0	🟪 Recycled	0	🟥 Readded	0

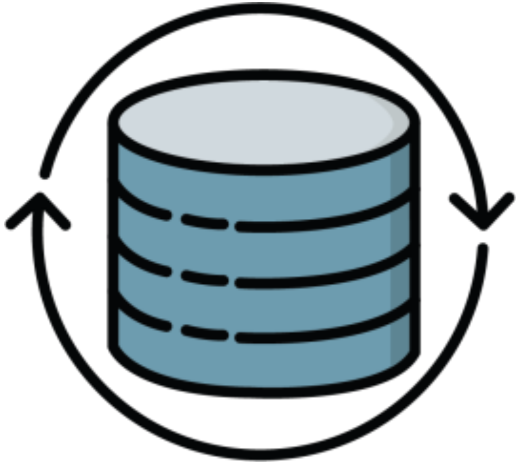
Full Backup : Initiated by Scheduler
Backup Date : 02-Sep-20 02:00
Time Taken : 28 secs
Status : success (Failed to backup c...

Explore backup

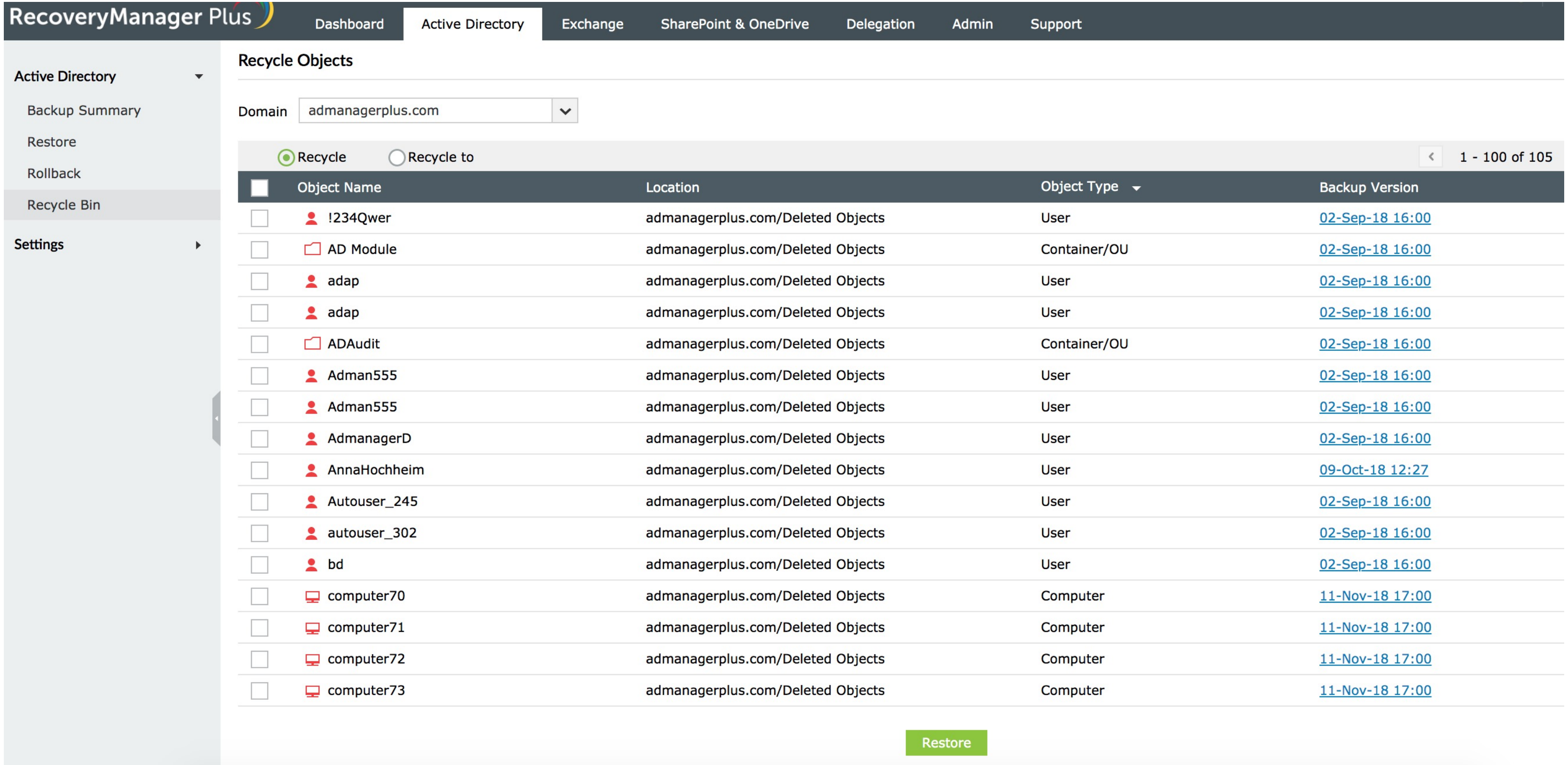
	User - 34	Computer - 3	Contact - 2	Group - 49	OU - 121	DNS Node - 0	DNS Zone - 0	GPO - 3	Site - 1	Dynamic Distri
Modified	-	-	-	-	-	-	-	-	-	-
Created	-	-	-	-	-	-	-	-	-	-
Added	34	3	2	49	121	-	-	3	1	-
Deleted	-	-	-	-	-	-	-	-	-	-
Moved	-	-	-	-	-	-	-	-	-	

AD備份還原 – 無需重啟還原

- 物件與屬性等級還原
- 無需重啟我們的網域控制器
- 支援Rollback與資源回收桶



使用情境 – 不小心刪到使用者，即時回覆


RecoveryManager Plus
Dashboard
Active Directory
Exchange
SharePoint & OneDrive
Delegation
Admin
Support
Active Directory
Backup Summary
Restore
Rollback
Recycle Bin
Settings
Restore

Recycle Objects

Domain admanagerplus.com

● Recycle ○ Recycle to

1 - 100 of 105

☐	Object Name	Location	Object Type	Backup Version
☐	!234Qwer	admanagerplus.com/Deleted Objects	User	02-Sep-18 16:00
☐	AD Module	admanagerplus.com/Deleted Objects	Container/OU	02-Sep-18 16:00
☐	adap	admanagerplus.com/Deleted Objects	User	02-Sep-18 16:00
☐	adap	admanagerplus.com/Deleted Objects	User	02-Sep-18 16:00
☐	ADAudit	admanagerplus.com/Deleted Objects	Container/OU	02-Sep-18 16:00
☐	Adman555	admanagerplus.com/Deleted Objects	User	02-Sep-18 16:00
☐	Adman555	admanagerplus.com/Deleted Objects	User	02-Sep-18 16:00
☐	AdmanagerD	admanagerplus.com/Deleted Objects	User	02-Sep-18 16:00
☐	AnnaHochheim	admanagerplus.com/Deleted Objects	User	09-Oct-18 12:27
☐	Autouser_245	admanagerplus.com/Deleted Objects	User	02-Sep-18 16:00
☐	autouser_302	admanagerplus.com/Deleted Objects	User	02-Sep-18 16:00
☐	bd	admanagerplus.com/Deleted Objects	User	02-Sep-18 16:00
☐	computer70	admanagerplus.com/Deleted Objects	Computer	11-Nov-18 17:00
☐	computer71	admanagerplus.com/Deleted Objects	Computer	11-Nov-18 17:00
☐	computer72	admanagerplus.com/Deleted Objects	Computer	11-Nov-18 17:00
☐	computer73	admanagerplus.com/Deleted Objects	Computer	11-Nov-18 17:00

案例分享

案例分享 – 華沙市政府/波蘭

- 既有狀態
  - 超過4,500網域使用者，只有40名網域管理員
- 遭遇問題
  - 管理員有超過30%的時間，在於協助重置密碼
  - 大量使用者在無法登入時，處於停擺狀態
  - 原生AD無法即時偵測網域遭到攻擊
- 導入後
  - 整個組織節省了20%的時間
  - 管理員可以更專注在資安議題上

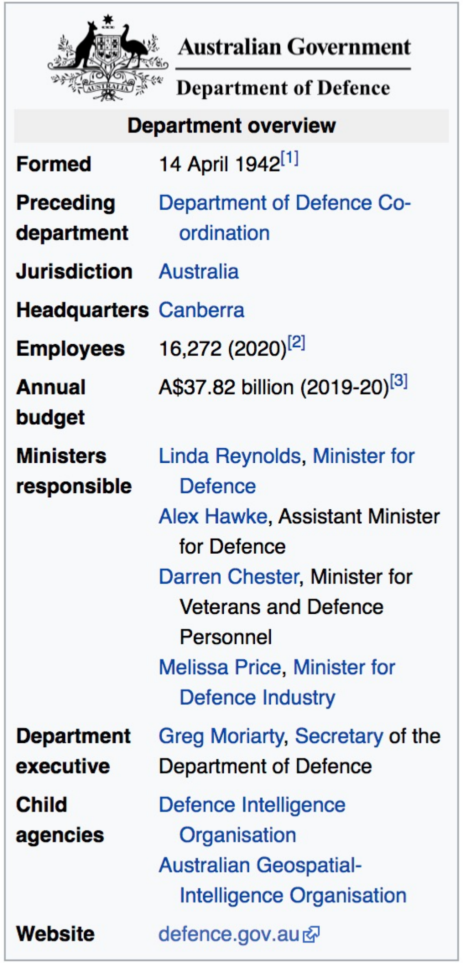
COMPANY: Warsaw City Hall

INDUSTRY: Government

LOCATION: Warsaw, Poland

案例分享 – 澳大利亞國防部/澳洲

- 各部門採用
  - CIO辦公室(Chief Information Officer Group.)
  - 網路整合中心(Land Network Integration Centre)
  - 水文服務局(Hydrographic Services)
- 採購服務
  - ITIL服務管理
  - AD管理
  - 桌面管理
  - 密碼管理等等



Australian Government
Department of Defence

Department overview	
Formed	14 April 1942[1]
Preceding department	Department of Defence Co-ordination
Jurisdiction	Australia
Headquarters	Canberra
Employees	16,272 (2020)[2]
Annual budget	A$37.82 billion (2019-20)[3]
Ministers responsible	Linda Reynolds, Minister for Defence Alex Hawke, Assistant Minister for Defence Darren Chester, Minister for Veterans and Defence Personnel Melissa Price, Minister for Defence Industry
Department executive	Greg Moriarty, Secretary of the Department of Defence
Child agencies	Defence Intelligence Organisation Australian Geospatial-Intelligence Organisation
Website	defence.gov.au

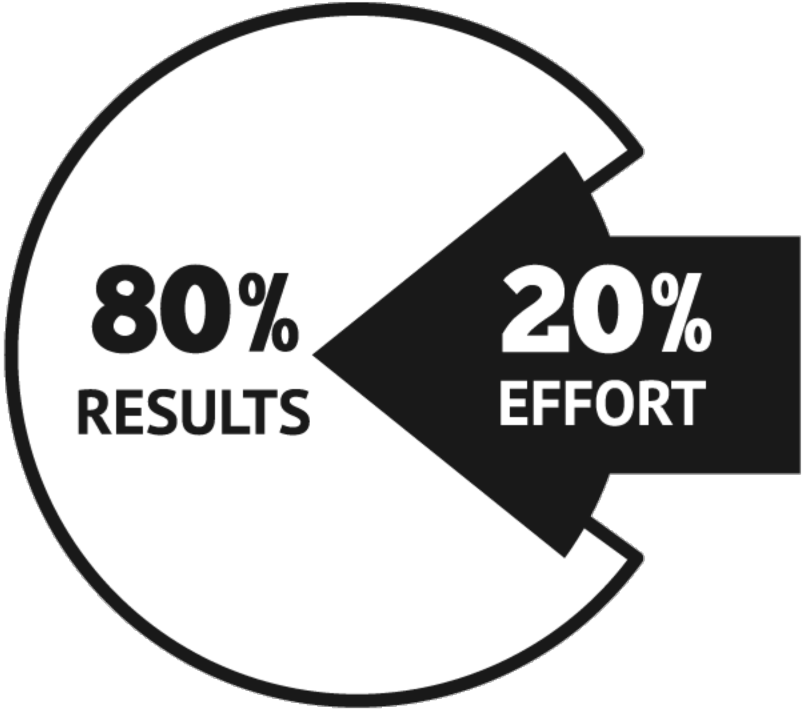
為你呈現

ManageEngine

Introduing ManageEngine

ManageEngine的概念就是

- 花更少的預算
- 得到相同的功能
- 甚至更多!


80%
RESULTS
20%
EFFORT

全方位IT管理解決方案

- IT整合管理
  - 提供 90 多種，價格合理，滿足您的所有 IT 管理需求之產品。
- IT簡化管理
  - 易於下載、安裝、設定和部署，無需第三方支援服務或幫助。
- IT實惠管理
  - 更高的價格並不始終意味著更好的產品

180,000+
家全球企業

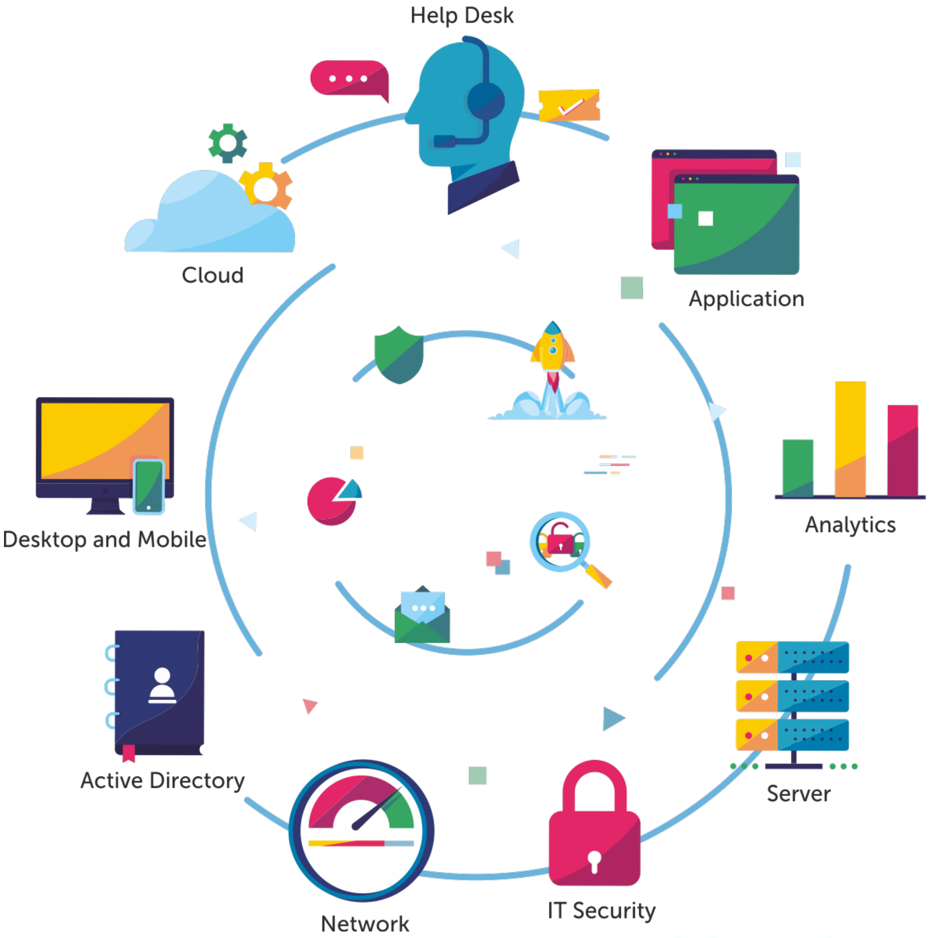
9/10
財富 100 強公司

3,000,000+
管理者

..信任 ManageEngine 來管理其 IT。

ManageEngine 協助您

- ITIL整合式資產和服務管理
- 更有效的管理雲平台
- 比讓微軟更實用的AD管理
- 大量端末設備
- 複雜的基礎設施
- 符合資安需求的稽核
- 可滿足所有IT管理需求


Help Desk
Application
Analytics
Server
IT Security
Network
Active Directory
Desktop and Mobile
Cloud

用更實惠的價格，滿足相同的需求

MICRO FOCUS

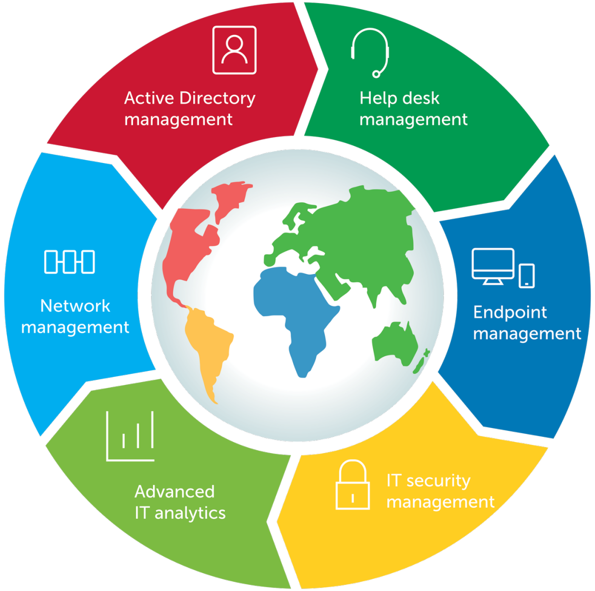
splunk>

netwrix

Quest

NETSCOUT

dynatrace

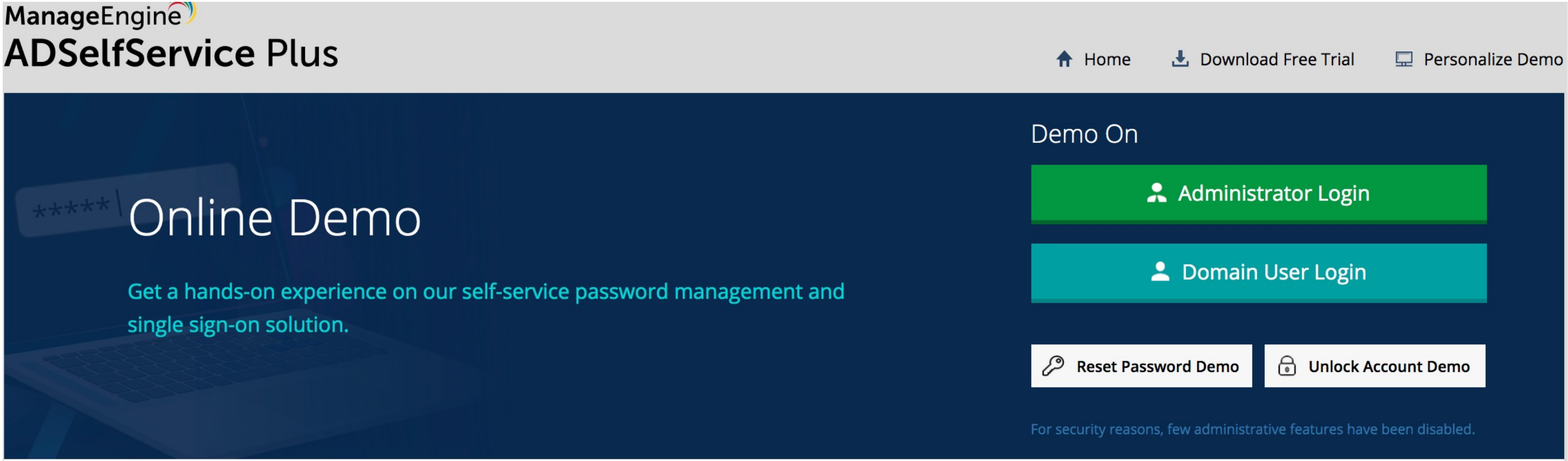

Active Directory management
Help desk management
Endpoint management
IT security management
Advanced IT analytics
Network management

您也可以選用

ManageEngine

每一項產品皆有線上DEMO

- 也可以申請30天 Trial License


ManageEngine

ADSelfService Plus

Online Demo

Get a hands-on experience on our self-service password management and single sign-on solution.

Demo On

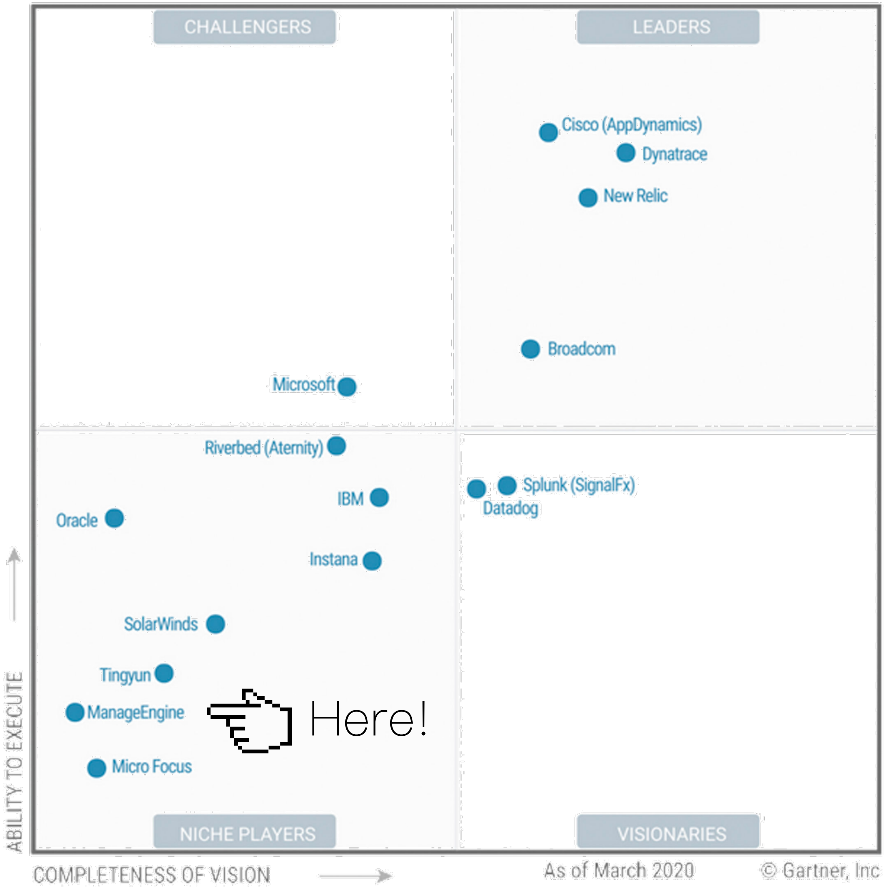
For security reasons, few administrative features have been disabled.

Home
Download Free Trial
Personalize Demo
*****
Administrator Login
Domain User Login
Reset Password Demo
Unlock Account Demo

入選各項Gartner魔術象限

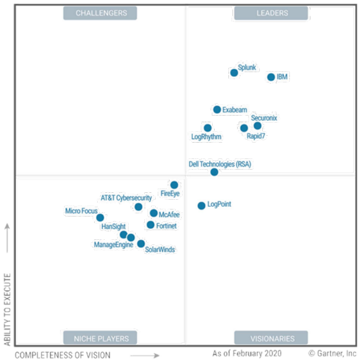
- 應用效能監控解決方案
- 連續八年

Figure 1. Magic Quadrant for Application Performance Monitoring



Source: Gartner (April 2020)

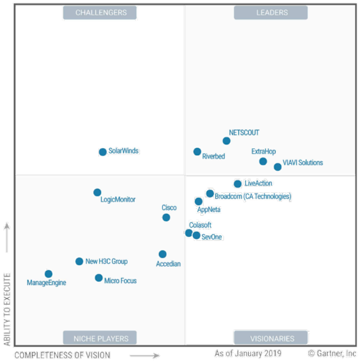
Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (February 2020)

Security Information
and
Event Management
(SIEM)
連續四年

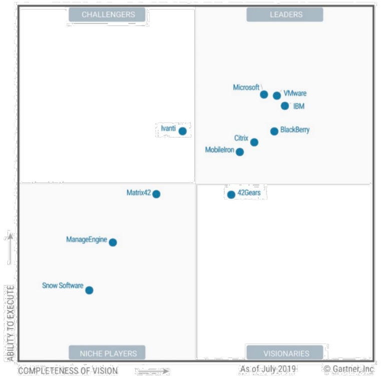
Figure 1. Magic Quadrant for Network Performance Monitoring and Diagnostics



Source: Gartner (February 2019)

Network Performance
Monitoring and Diagnostics
(NPMD)
連續兩年

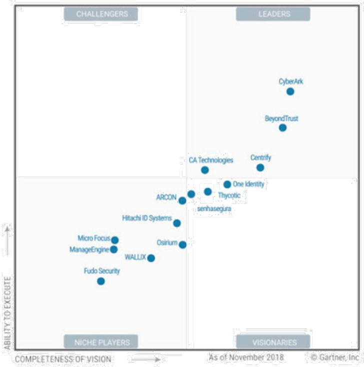
Figure 1. Magic Quadrant for Unified Endpoint Management



Source: Gartner (August 2019)

Unified Endpoint
Management Tools.
(UEM)
連續兩年

Figure 1. Magic Quadrant for Privileged Access Management



Source: Gartner (December 2018)

Privileged
Access
Management
(PAM)

獲獎無數的整合解決方案

PINK

Gartner®

STRONG VALUE
Zoho/ManageEngine
EMA Radar™ for
Mobile Device Management 2016

FORRESTER®

SC MAGAZINE ★★★★★

IDC
Analyze the Future

THE INTEGRATOR
ict CHAMPION AWARDS

VENDOR LANDSCAPE AWARD
BEST OVERALL VALUE
INFO~TECH research group

EMA™

Redmond
READER'S CHOICE AWARDS
2015

全球各大企業指定使用

at&t
L'ORÉAL PARIS
BARCLAYS
SONY
GE
SAINT-GOBAIN
ERICSSON TAKING YOU FORWARD
NEC

Alcatel-Lucent
TIME WARNER CABLE
Digicel PNG's Bigger, Better Network.
ABN·AMRO
DHL
HUGHES NETWORK SYSTEMS
U21Global Graduate School For Global Leaders
AOL

NOKIA Connecting People
Seagate
EDS
Hallmark
MetLife
cellnet
City of Seattle Department of Neighborhoods
AIRBUS

Lufthansa
بنك أبوظبي التجاري ADCB
NAVY.mil
Los Alamos National Bank Creating a better way.
UCLA
USGS science for a changing world
Infosys
ERNST & YOUNG Quality In Everything We Do

Ogilvy
IBM
SADDLE CREEK CORPORATION
TATA CONSULTANCY SERVICES
comviva Beyond Boundaries
TULIP making it possible
Kryptos
HCL

TD Waterhouse Wealth of Experience
SIEMENS
TATA
Fidelity INVESTMENTS
MICHIGAN
intel
BRITISH AMERICAN TOBACCO
Reliance Industries Limited

IKEA
HONDA The Power of Dreams
18 78 Everton
BRIDGESTONE
OXFORD UNIVERSITY PRESS
xerox
unicef
TOSHIBA Leading Innovation

CHS
Symantec
NORTHROP GRUMMAN
L&T Infotech
CISCO

選擇ManageEngine

- 易於安裝、易於操作、易於管理
- 與企業一同成長，彈性增長規格
- 極具競爭力的價格

THANK YOU

Any Questions?
Or
Contact Kerry