# SmartThink

Introduction to Information Security

# INFORMATION SECURITY CONCEPTS

- **Management direction for information security:**
  - An information security (IS) policy is **a set of rules and guidelines that dictate how information technology (IT) assets and resources should be used, managed, and protected**. It applies to all users in an organization or its networks as well as all digitally stored information under its authority.
  - Developing an Information Security policy is to ensure the **Confidentiality**, **Integrity** and **Availability** of information systems.
  - All developed Information Security policies should be reviewed on a regular basis to ensure they meet the organizations objectives.
  - Examples of information security policies are:
    - Email Use Policy
    - Acceptable Use Policy
    - User Access Policy
    - Data disposal Policy
    - Network Use and Firewall Policy

# Roles and Responsibilities

- For the information security unit/organization to function, several roles and responsibilities need to be defined. Several parties play an important role in ensuring the successful of the information security units. They include:
  - Board of Directors
  - Management
  - Cyber Security Strategy Committee
  - Chief Information Security Officer (CISO)
  - Information Security Compliance Officer
  - Information Security Architect
  - Information Security Analyst
  - Information Security Audito.

# Human Resource Security

- What is human resource security?
  - Human Resource Security is a set of processes designed to ensure that all **employees**, **suppliers**, and **contractors** are qualified for and understand their engagement/job tasks and responsibilities, and that access is revoked after the engagement is finished.
  - Human resource security is broken down into 3 distinct processes:
    - Processes before employment/onboarding
    - Processes to ensure that employees and contractors fulfil their information security responsibilities
    - Processes for termination and change of employment

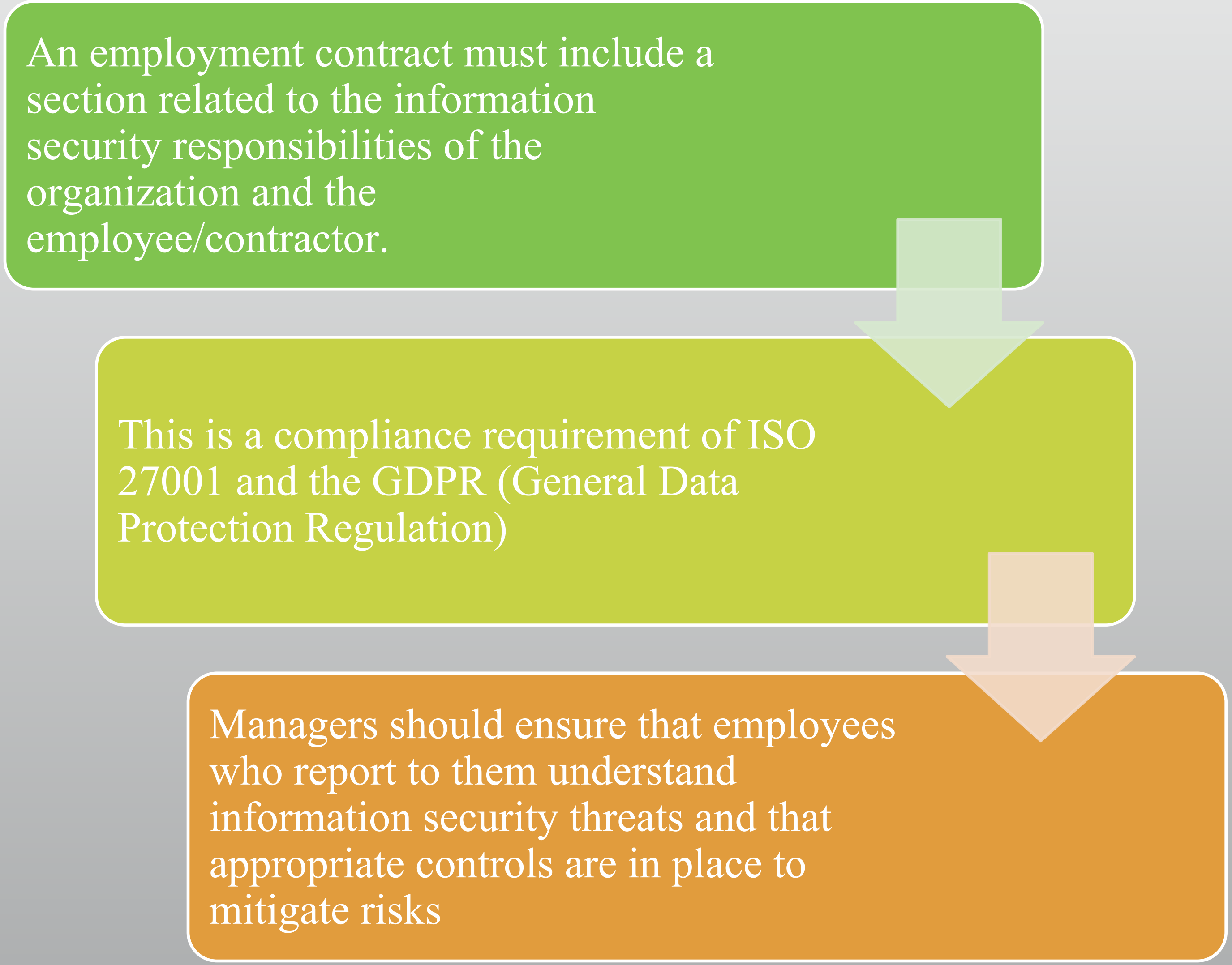
# Screening

Employees / Contractors screening is the process of verifying an applicant’s credentials and ensuring that they meet the conditions for employment/contract.

The screening process should, for example, establish whether the applicant has concealed or falsified information, such as their qualifications and job history.

Applicants whose jobs involve accessing sensitive information should be subject to more extensive screening.

# Terms and conditions of employment



An employment contract must include a section related to the information security responsibilities of the organization and the employee/contractor.

This is a compliance requirement of ISO 27001 and the GDPR (General Data Protection Regulation)

Managers should ensure that employees who report to them understand information security threats and that appropriate controls are in place to mitigate risks

# Information Security Awareness Training

Employees and relevant contractors must receive information security staff awareness training.

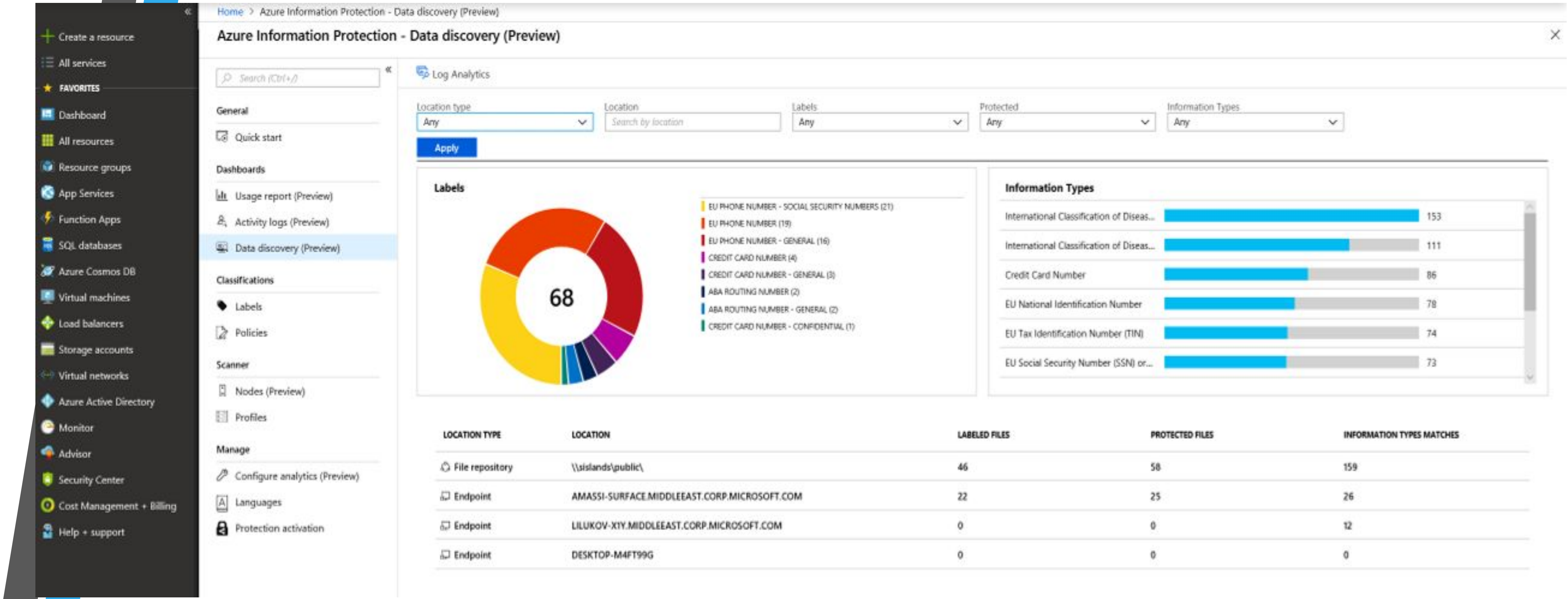
These training courses should be retaken at regular intervals to refresh employees’ knowledge and account for changes in how the organisation operates

# Termination or change of employment responsibilitie s

- When an employee leaves their job through termination or voluntarily due to or changed roles they are supposed to know their information security responsibilities.
- For example, they are still expected to protect confidential information, and they are prohibited from keeping sensitive information belonging to the employer.
- Organizations must define the responsibilities that come with the termination of or change in employment, communicate them to the employee and make sure they are enforced.
- Additionally, there are steps that employees must take when they leave their role, such as returning company equipment and keys, fobs, passes, etc. to the premises.
- Another example, if an employee moves to a different department, the organisation must ensure that they no longer have access to information assets that aren’t required for their new role.

# Asset Management

- Cybersecurity asset management is the process of identifying, on a continuous, real-time basis, the IT assets that your organization owns and the potential security risks or gaps that affect each one. In this context, assets take many forms. They could be traditional devices, like PCs and servers, data, human resources etc.



Home > Azure Information Protection - Data discovery (Preview)

Azure Information Protection - Data discovery (Preview)

Location type: Any
Location: Search by location
Labels: Any
Protected: Any
Information Types: Any

**Labels**

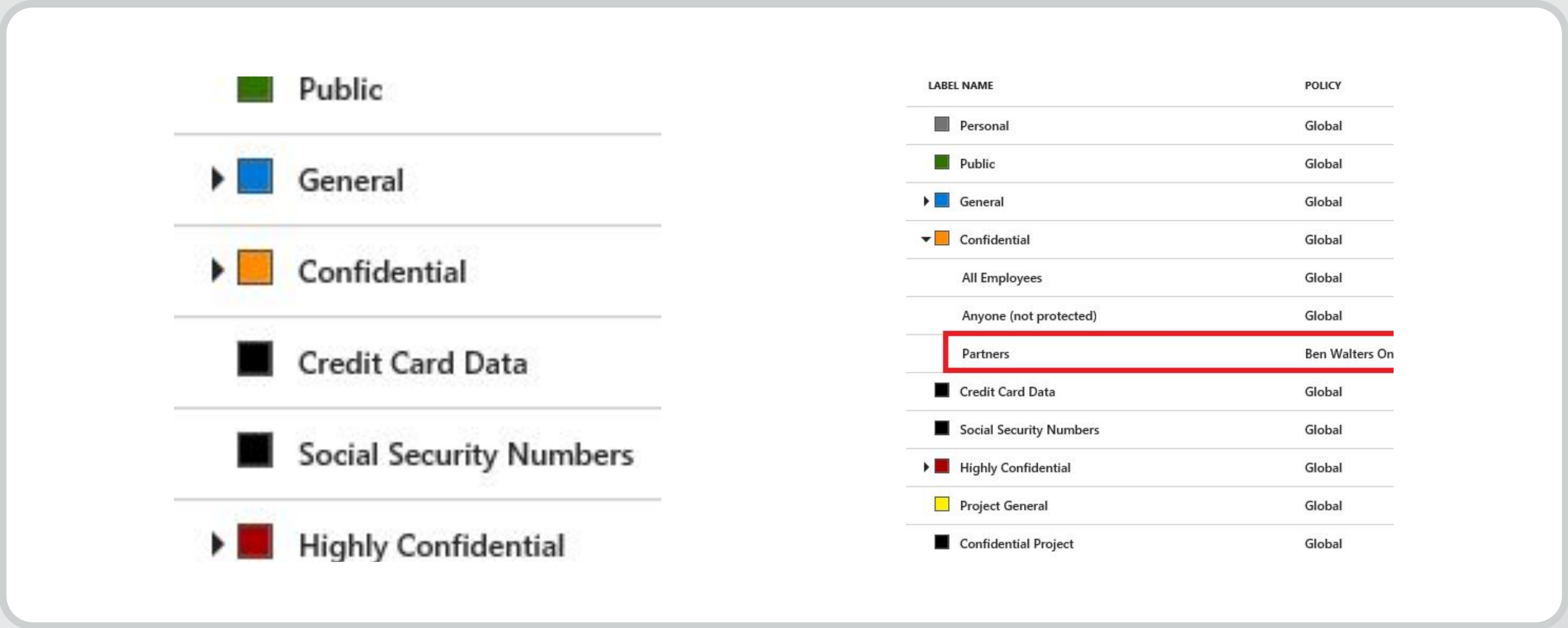
68

- EU PHONE NUMBER - SOCIAL SECURITY NUMBERS (21)
- EU PHONE NUMBER (19)
- EU PHONE NUMBER - GENERAL (16)
- CREDIT CARD NUMBER (4)
- CREDIT CARD NUMBER - GENERAL (3)
- ABA ROUTING NUMBER (2)
- ABA ROUTING NUMBER - GENERAL (2)
- CREDIT CARD NUMBER - CONFIDENTIAL (1)

**Information Types**

| | |
|---|---|
| International Classification of Diseas... | 153 |
| International Classification of Diseas... | 111 |
| Credit Card Number | 86 |
| EU National Identification Number | 78 |
| EU Tax Identification Number (TIN) | 74 |
| EU Social Security Number (SSN) or... | 73 |

| LOCATION TYPE | LOCATION | LABELED FILES | PROTECTED FILES | INFORMATION TYPES MATCHES |
|---|---|---|---|---|
| File repository | \\sislands\public\ | 46 | 58 | 159 |
| Endpoint | AMASSI-SURFACE.MIDDLEEAST.CORP.MICROSOFT.COM | 22 | 25 | 26 |
| Endpoint | LILUKOV-X1Y.MIDDLEEAST.CORP.MICROSOFT.COM | 0 | 0 | 12 |
| Endpoint | DESKTOP-M4FT99G | 0 | 0 | 0 |



- 🟩 Public
- ▸ 🟦 General
- ▸ 🟧 Confidential
- ⬛ Credit Card Data
- ⬛ Social Security Numbers
- ▸ 🟥 Highly Confidential

| LABEL NAME | POLICY |
|---|---|
| ◼ Personal | Global |
| 🟩 Public | Global |
| ▸ 🟦 General | Global |
| ▾ 🟧 Confidential | Global |
| All Employees | Global |
| Anyone (not protected) | Global |
| Partners | Ben Walters On |
| ⬛ Credit Card Data | Global |
| ⬛ Social Security Numbers | Global |
| ▸ 🟥 Highly Confidential | Global |
| 🟨 Project General | Global |
| ⬛ Confidential Project | Global |

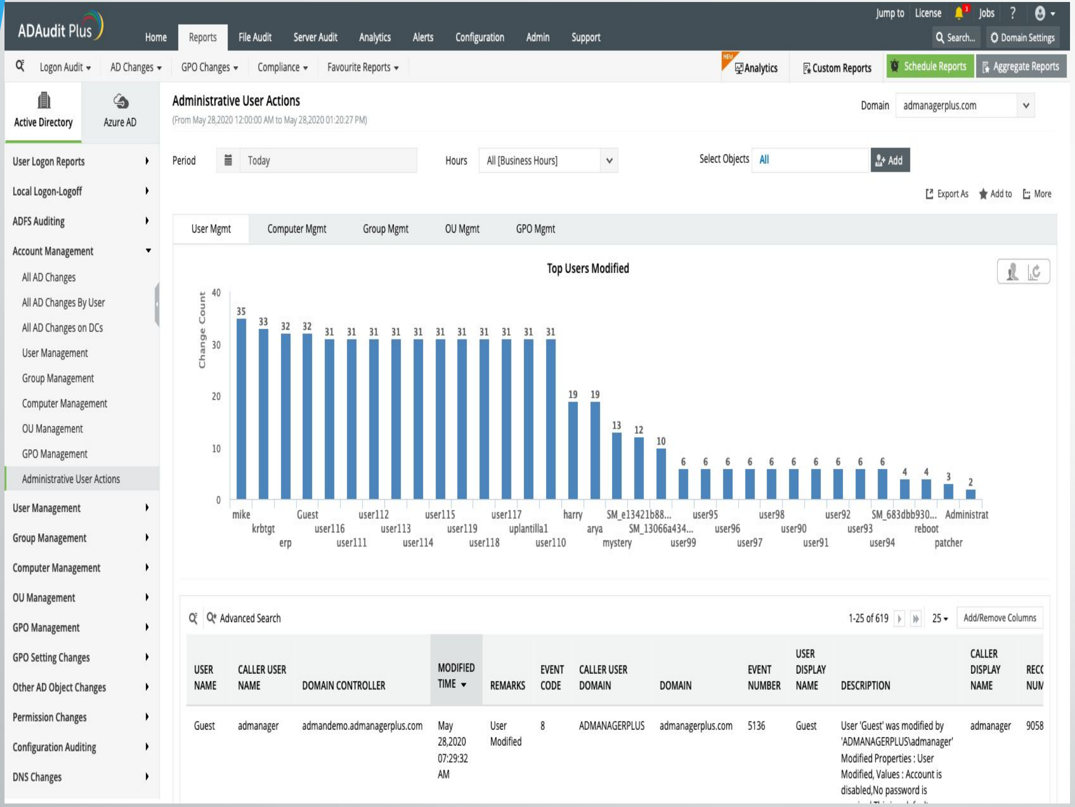
# Information Classification

# Access Control

- Access control is an essential element of security that determines who is allowed to access certain data, applications, and resources—and in what circumstances. In the same way that keys and preapproved guest lists protect physical spaces, access control policies protect digital spaces. In other words, they let the right people in and keep the wrong people out. **Access control policies** rely heavily on techniques like authentication and authorization, which allow organizations to explicitly verify both that users are who they say they are and that these users are granted the appropriate level of access based on context such as device, location, role, and much more.

- Access control keeps **confidential** information—such as customer data and intellectual property—from being stolen by bad actors or other unauthorized users. It also reduces the risk of data exfiltration by employees and keeps web-based threats at bay. Rather than manage permissions manually, most security-driven organizations lean on identity and access management solutions to implement access control policies.

# Identity and Access Management (IAM)



Administrative User Actions

(From May 28,2020 12:00:00 AM to May 28,2020 01:20:27 PM)

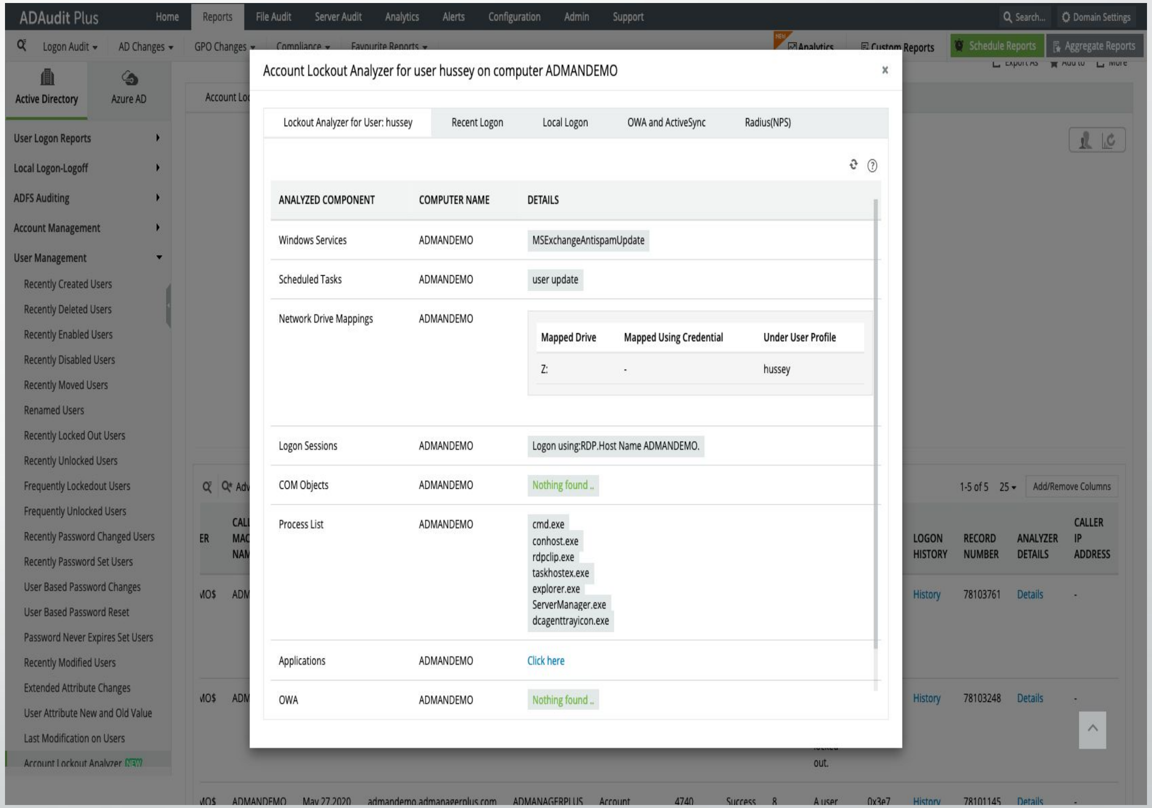
Domain: admanagerplus.com

Period: Today

Hours: All [Business Hours]

Select Objects: All

| USER NAME | CALLER USER NAME | DOMAIN CONTROLLER | MODIFIED TIME ▾ | REMARKS | EVENT CODE | CALLER USER DOMAIN | DOMAIN | EVENT NUMBER | USER DISPLAY NAME | DESCRIPTION | CALLER DISPLAY NAME | RECC NUM |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Guest | admanager | admandemo.admanagerplus.com | May 28,2020 07:29:32 AM | User Modified | 8 | ADMANAGERPLUS | admanagerplus.com | 5136 | Guest | User 'Guest' was modified by 'ADMANAGERPLUS\admanager' Modified Properties : User Modified, Values : Account is disabled,No password is | admanager | 9058 |



Account Lockout Analyzer for user hussey on computer ADMANDEMO ×

Lockout Analyzer for User: hussey | Recent Logon | Local Logon | OWA and ActiveSync | Radius(NPS)

| ANALYZED COMPONENT | COMPUTER NAME | DETAILS |
|---|---|---|
| Windows Services | ADMANDEMO | MSExchangeAntispamUpdate |
| Scheduled Tasks | ADMANDEMO | user update |
| Network Drive Mappings | ADMANDEMO | Mapped Drive: Z:<br>Mapped Using Credential: -<br>Under User Profile: hussey |
| Logon Sessions | ADMANDEMO | Logon using:RDP.Host Name ADMANDEMO. |
| COM Objects | ADMANDEMO | Nothing found .. |
| Process List | ADMANDEMO | cmd.exe<br>conhost.exe<br>rdpclip.exe<br>taskhostex.exe<br>explorer.exe<br>ServerManager.exe<br>dcagenttrayicon.exe |
| Applications | ADMANDEMO | Click here |
| OWA | ADMANDEMO | Nothing found .. |

Thank you

# Any Questions?