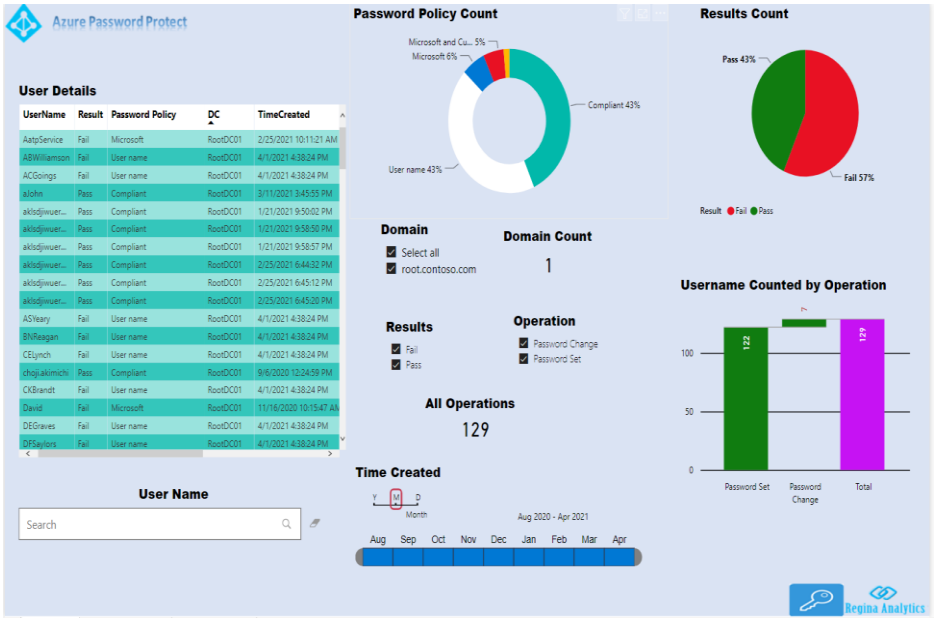
Regina Analytics



Azure AD Password Protection for Active Directory Domain Services with PowerBI reporting

OVERVIEW

Azure Active Directory Protection for Active Domain uses Microsoft curated list to scan for weak passwords, give a report for the weak password with addition of PowerBI.

Michael Mutekeri
Data Scientist

Introduction

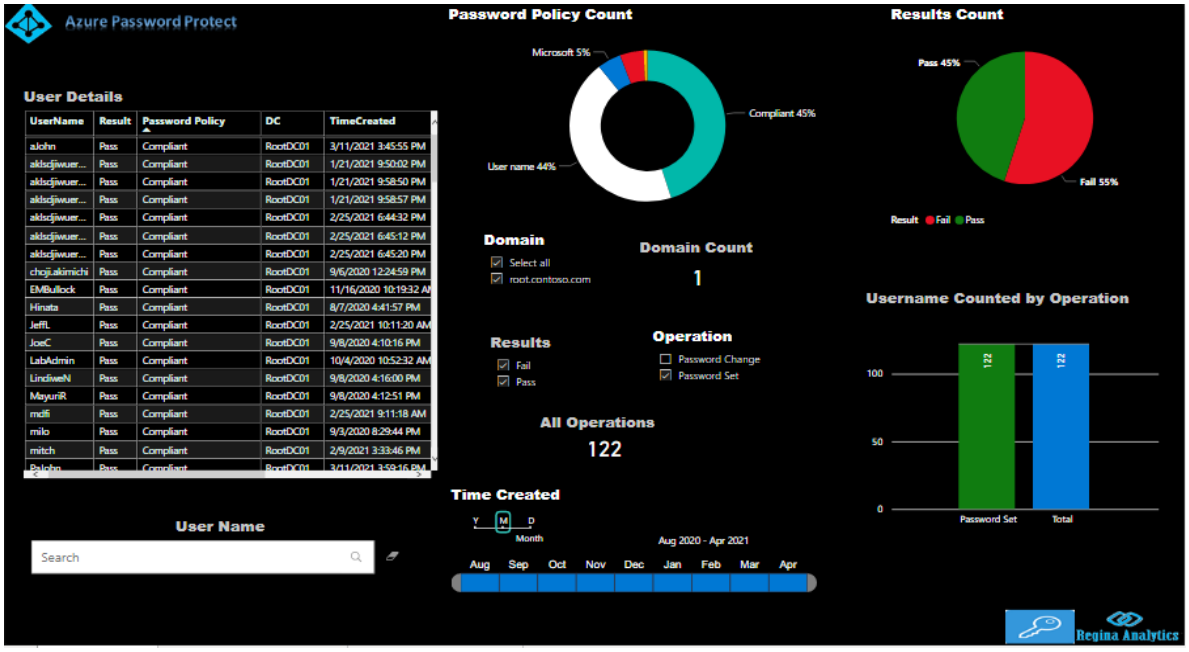


Figure 1: Dark mode

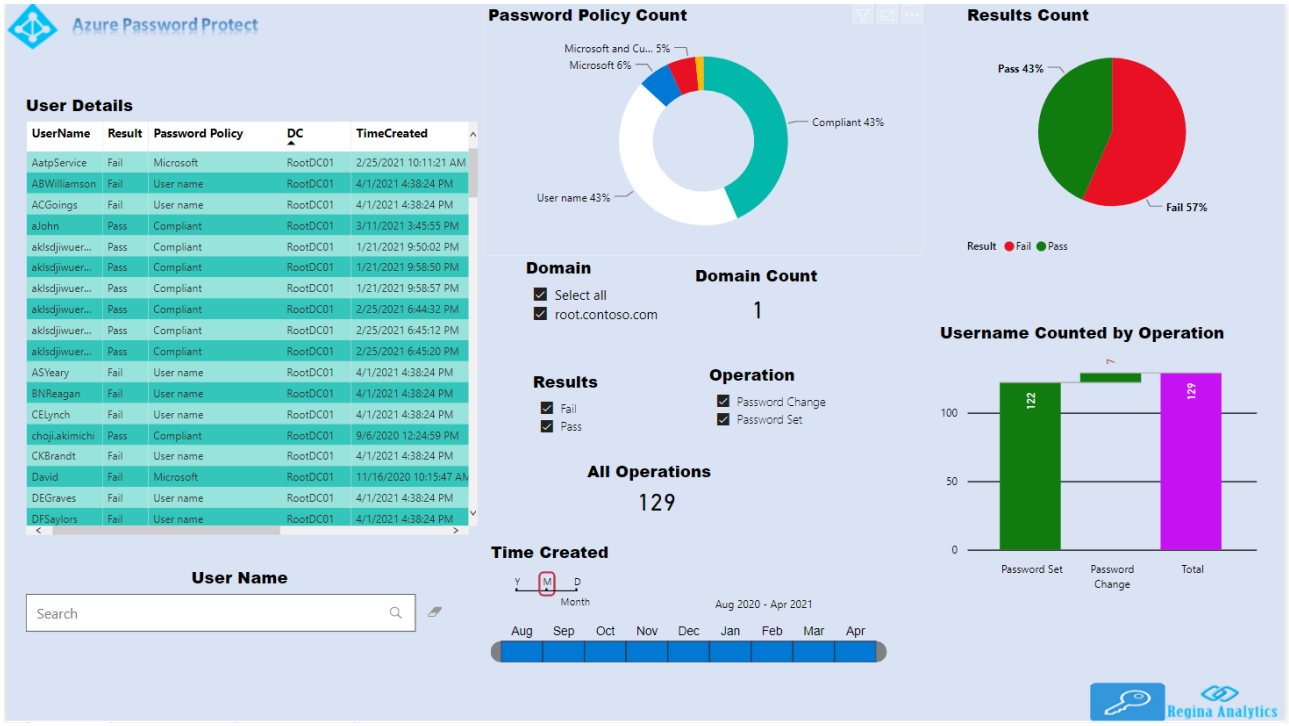


Figure 2: Light mode

As a service company we are looking for ways to find our customers the best way to operate on the most secure service. As we all know, most people use the Microsoft suite service and with the exciting news of cloud services, we are all using azure services one way or another. Through simple solutions like Microsoft 365 suite.

- Have you thought as a manager, how secure are passwords on your premises?
- How do you guard against spray attacks from hackers?

Azure Active Directory Protection for Active Domain uses Microsoft curated list to scan for weak passwords, give a report for the weak password. The customer can use a custom list in addition, according to the organisation culture on common passwords in addition to the audit.

Acronym

ADDS	- Active Directory Domain Services
Azure AD	- Azure Active Directory
DC	- Domain Controller

Background

Azure AD Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization. On-premises deployment of Azure AD Password Protection uses the same global and custom banned password lists that are stored in Azure AD, and does the same checks for on-premises password changes as Azure AD does for cloud-based changes. These checks are performed during password changes and password reset events against on-premises Active Directory Domain Services (AD DS) domain controllers. The service already exists on the Azure service, given that the customer has license for Premium P1 or Premium P2 and is running a hybrid architecture. The customer will need to activate the service and deploy solution.

Requirements

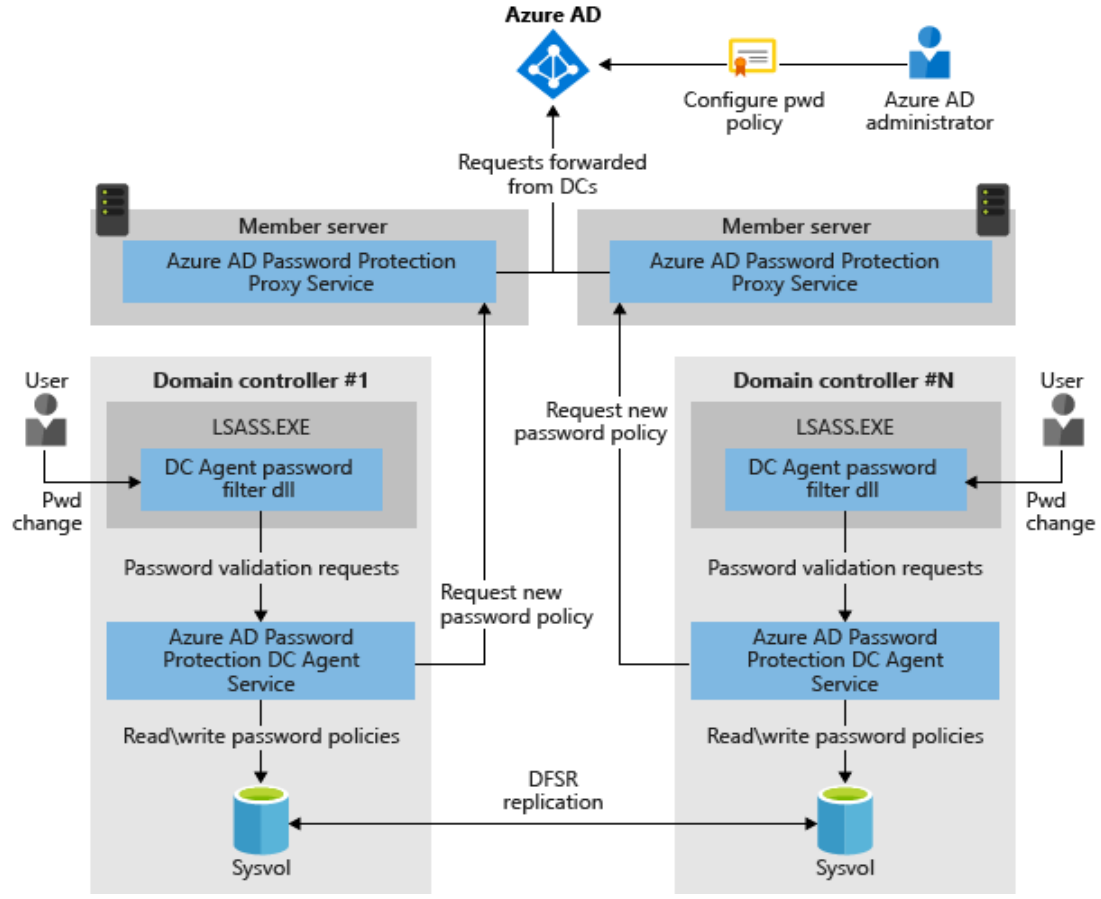


Figure 3: Architecture

License Requirements

1. The customer must already be subscribing to Azure services
2. The customer must have either Premium P1 or Premium P2 package
3. The customer must have a hybrid infrastructure with Azure services for both on-premises and cloud
4. On-premises AD DS users that are not synchronized to Azure AD also benefit from Azure AD Password Protection based on existing licensing for synchronized users.
5. PowerBI license with free or paid version for dashboard

Users	**Azure AD Password Protection with global banned password list**	**Azure AD Password Protection with custom banned password list**
Cloud-only users	Azure AD Free	Azure AD Premium P1 or P2
Users synchronized from on-premises AD DS	Azure AD Premium P1 or P2	Azure AD Premium P1 or P2

Table 1: License requirements

Hardware requirements

6 Since your DCs never talk directly with Azure you need at least 2 Azure AD Password Protection Proxy Servers per Forest for high availability and should be placed in the Root Domain. The Azure AD Password Protection Proxy Servers must be Windows Server 2012R2 or above.

Procedures

7 Download the Azure AD Password Protection software

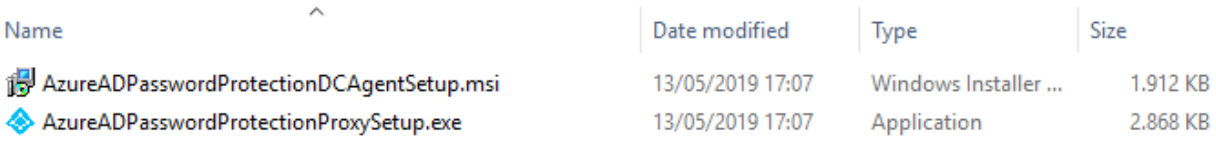


Figure 4:Installation

System operation

Audit mode - scans the passwords according to current policies and identifies unsecured password. The customer will make a decision according to statistics of the number of unfit vs fit passwords.

Enforce mode - ban all unsecured passwords as a customer try to make them.

Our services

I Assess existing architecture and recommend
II Deploy and configure the solution according to Microsoft best practices
III Help in creating a custom password list
IV Running workshops:
- User training
- supporting the solution
- Usage

V PowerBI reporting
VI Consult on the overall process

Microsoft PowerBI Dashboard solution for better visualisation and analysis

Basic reporting is available in tabular forms, with the enhancement of a Microsoft PowerBI reporting tool more information can be extracted in the form of graphics, it works on both paid and free versions.

Features

I. Gives a status of weak passwords on the domain
II. Gives a compliance report according to the Microsoft curated list
III. Identifies weak passwords
IV. Monitors users' activities on changes and resetting a password
V. A continuous automated report, that updates regularly

Training and awareness program

After the first audit, depending on the result. The customer can opt for training of staff on awareness on how to create secure passwords and the implications on security for unsecured passwords, including basic technical support for the technical team.

Price

R26000

Process

- Assessment
- Deployment (audit mode)
- Workshops
- PowerBI reporting
- Enforce mode