User Manual

Hybrid IT Management Framework

Document Revision History

Project Name: Hybrid IT Management Framework – User Manual

Document Status: Final

Document Version	Date	Prepared / Modified by	Reviewed by	Approved by	Section and Text Revised
1.0	20 May 2021	Sien Van Broekhoven	Dries Verschaeve		Full document

Table of Contents

Introduction

This document will serve as a user manual for users and administrators in an environment that's built based on the Hybrid IT Management Framework solution. This document will be split into different parts, each part representing a guide for a specific group of people (users, administrators, security operators).

This guide will describe the specific actions different users can do. This guide will not describe how to create new users or assign permissions to user, this is described in the installation manual.

1. Users

This segment contains the manual for regular users in the environment. “Regular users” means users that do not have any special privileges on top of the basic enterprise privileges. These users are able to use client computers in the environment, browse the internet, access enterprise applications (that are made available to them by administrators), and do other general non-privileged tasks.

Users will be able to log onto client computers in the environment with their domain account and password. The domain account to log onto computers consists of “domain/user”, an example from my lab environment is “stagesien/Alex”.

If this user wants to login to services offered to them, such as the Microsoft Azure portal, they can log in with their username in the following format: “username@domain.com”, an example from my lab environment: Alex@stagesien.onmicrosoft.com. The password for these services will be the same as the password they use to log in on a computer.

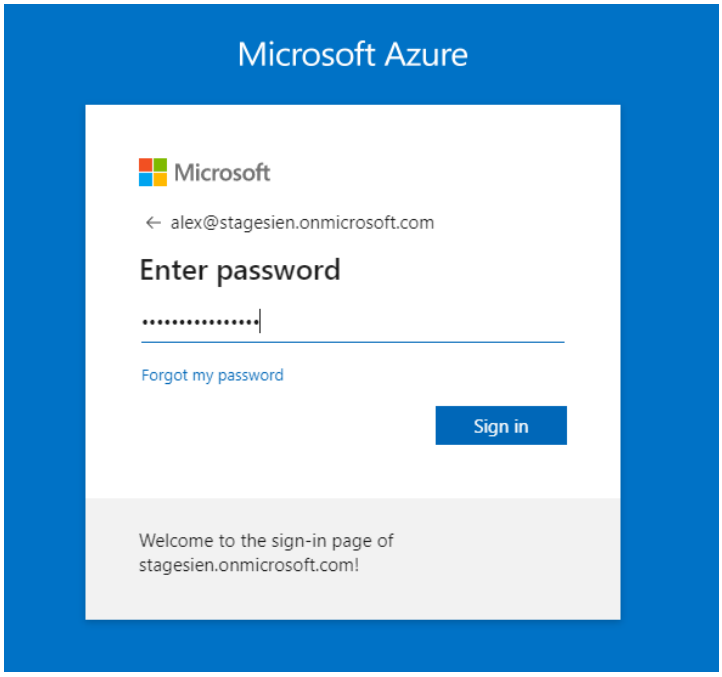

Figure 1: Microsoft Azure login screen

Note
The .onmicrosoft domain is a domain that acts as a unique identifier and is also used for mail routing purposes. However most organizations will use their own registered domain address instead.

Multi factor authentication (MFA) is enabled for all users in the environment. When a user first logs into a Microsoft service, they will have to fill in some information to properly configure MFA for this user. The user can choose from different authentication methods such as security questions, SMS, a mobile app code, or an email.

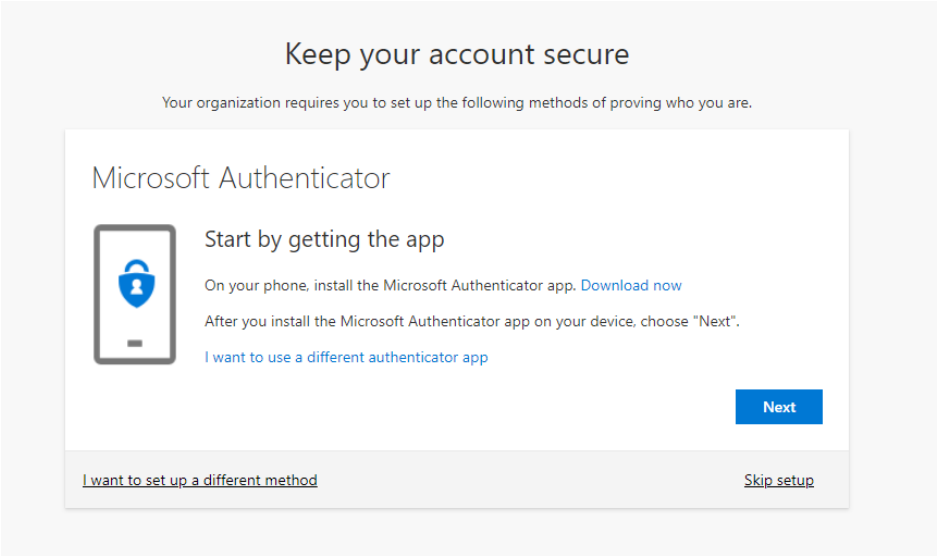

Figure 2: Mulitple Factor Authentication

If a user forgets their password, they can reset it themselves without the need for contacting an administrator. This is only possible if the Self Service Password Reset solution is enabled in Azure AD by an administrator, like described in the installation manual.

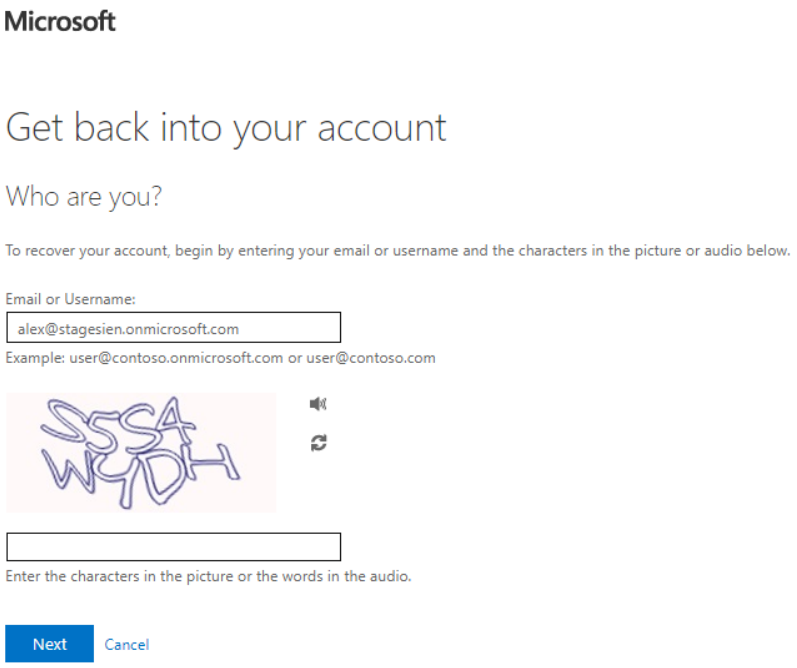

Figure 3: Self service Password Reset

Note
In an organization with an already existing on-premises environment, users most likely already exist. These users will be migrated to the Azure AD cloud environment through Azure AD Connect Sync. When the users are migrated, they can make use of the Cloud services.

2. Administrators

In every organization there are different types of administrators. The amount of administrative accounts and which specific roles and privileges these accounts have, is different per organization.

Custom administrator accounts can be created by domain administrators in Microsoft Active Directory.

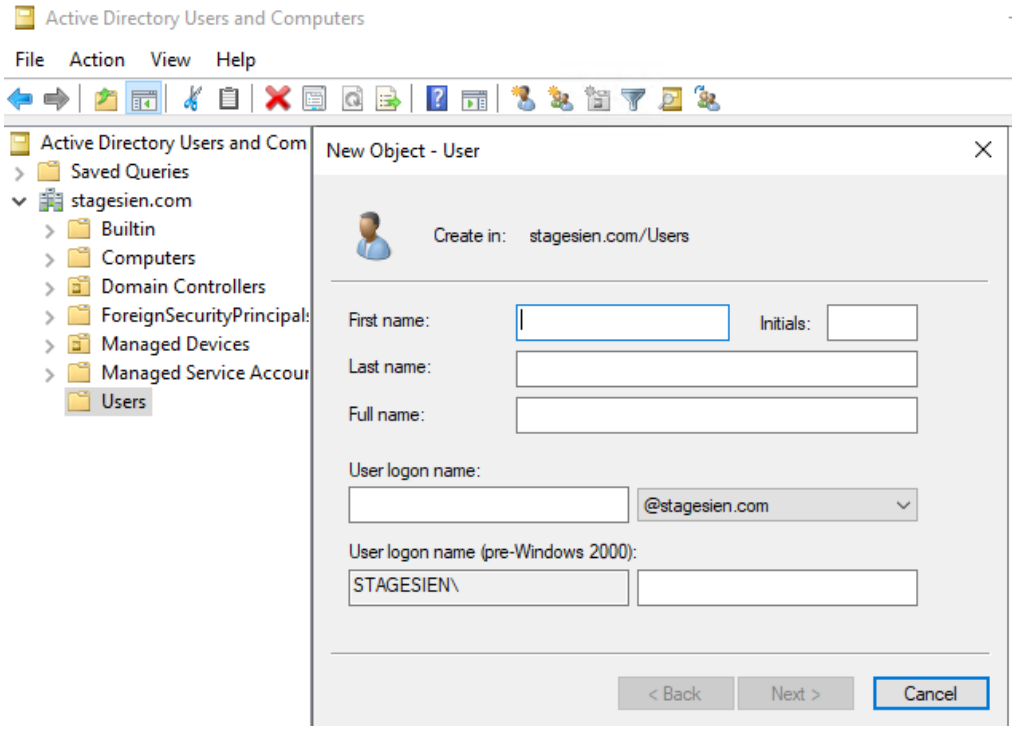

Figure 4: New Active Directory administrator account

Cloud administrator accounts can be created by users with user administrator or global administrator privileges in Azure AD. A full overview of all built-in Azure Active Directory roles can be found here.

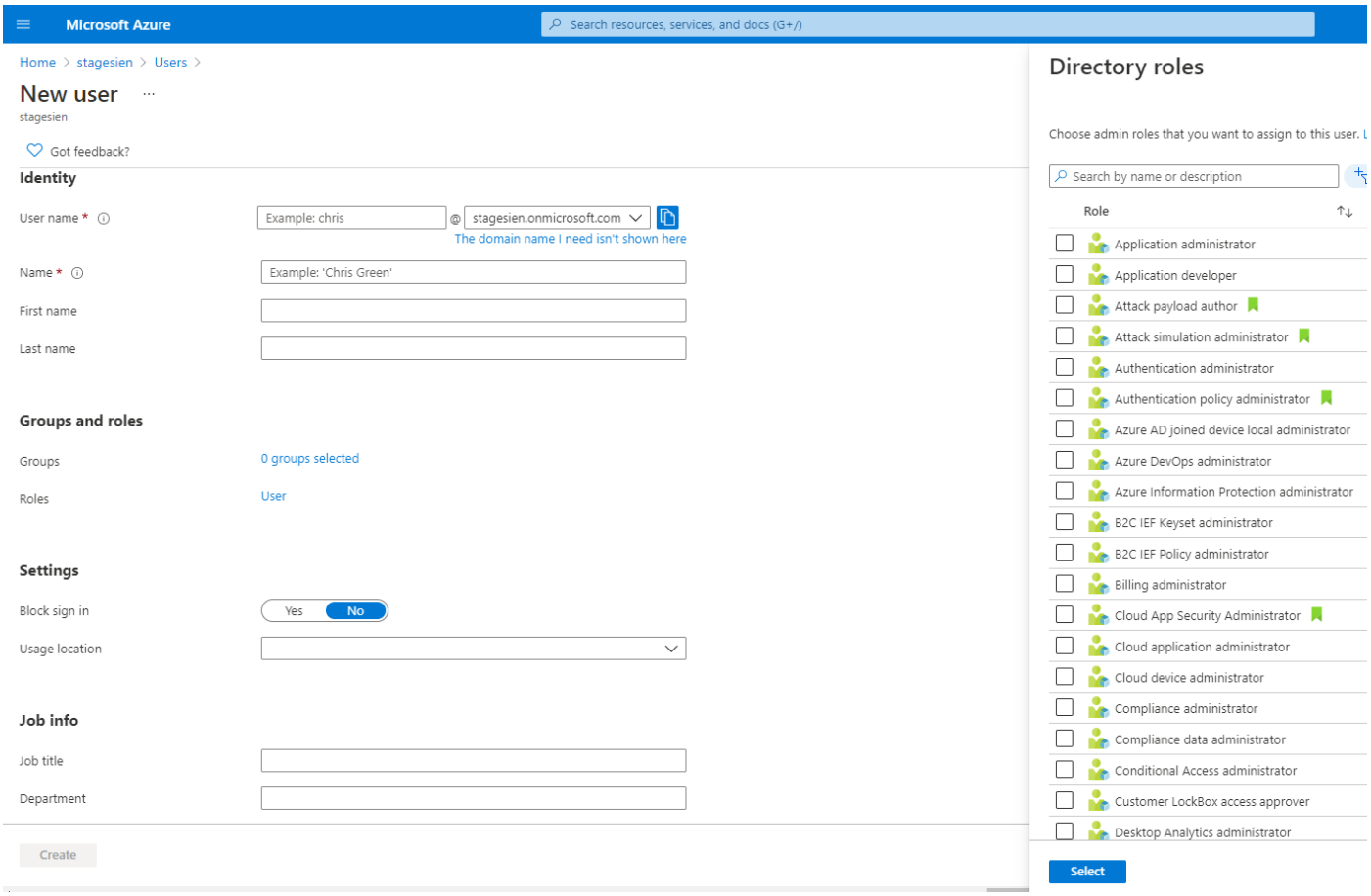

Figure 5: New Azure Active Directory administrator account

In this segment, a few different types of administrative accounts and roles will be described, including how to use these accounts. Only the more commonly used administrator accounts will be described, the link in the paragraph above provides more information about other administrative accounts.

Enterprise Administrator

The enterprise administrator group is an Active Directory built-in group that gets created when creating a new Active Directory forest. Accounts in this group have the highest privileges and should only be used when absolutely necessary, for example when creating a new domain in the forest.

Note

The enterprise administrator group is not synced to the Azure AD cloud. Users have to be added to this group in the on-premise Active Directory. The users that are added to this group can be synced to Azure AD, but as a best practice this should be avoided for safety precautions and only be allowed when absolutely necessary.

Enterprise admin accounts by default have access to all the machines in an active directory forest through RDP and WinRM, if these ports are open on the machine. The installation manual includes a guide on how to secure WinRM and RDP ports for machines, with a way to restrict these connections to only be allowed when they come from the ManagementVMs.

If an enterprise administrator wants to make configurations in the Active Directory environment/forest, they can connect to a domain controller through the Windows Admin Center interface. This interface can be opened in a browser window on any client computer in the environment, the enterprise admin should log onto this client computer with a regular user account. The Windows Admin Center (WAC) interface can be opened by typing in the url, which should be the fully qualified domain name of the server on which WAC is being hosted. If WAC is being hosted on multiple servers which form a cluster, then this url will use the cluster hostname. This interface will present a login screen, in which the enterprise admin should log in to with an account with enterprise administrator privileges.

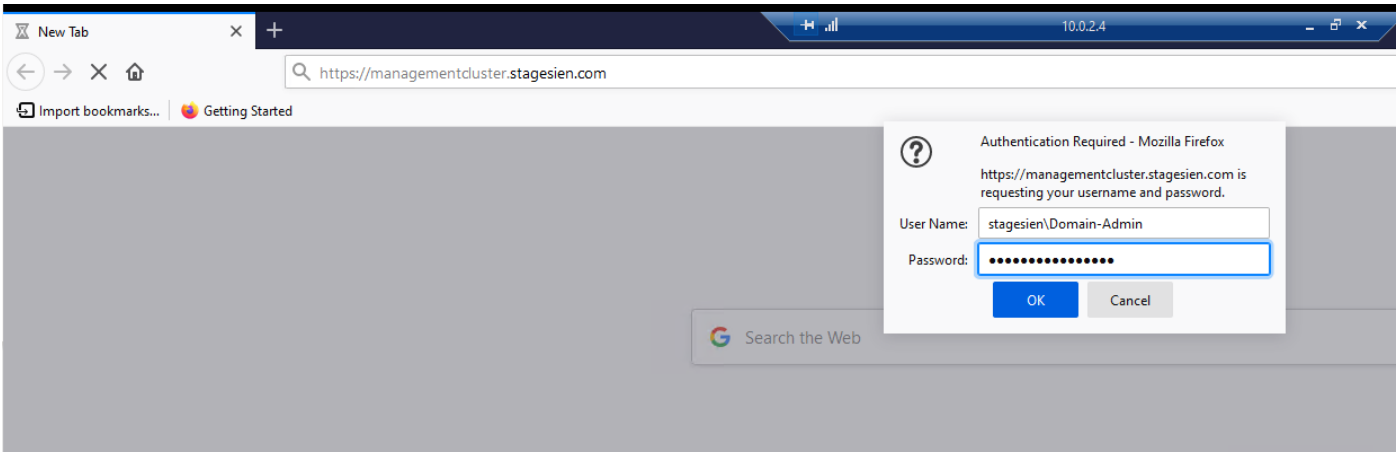

Figure 6: Windows Admin Center login screen

In Windows Admin Center the administrator can connect to all the servers and machines of the environment. To make AD forest configurations the administrator can use the Remote PowerShell or Remote Desktop Protocol option on the domain controllers, which will open a connection to manage the domain controller.

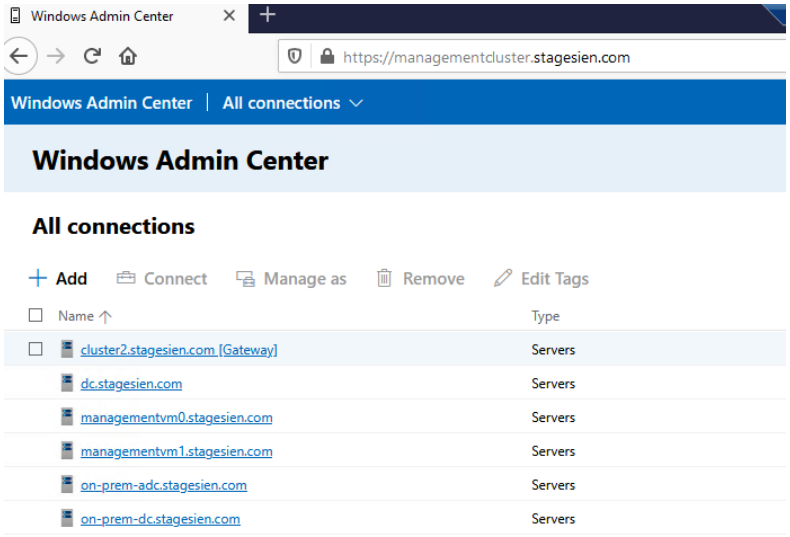

Figure 7: Windows Admin Center interface

Direct RDP and WinRM connections to critical systems such as domain controllers are restricted to only allow incoming connections from the ManagementVMs. Even an enterprise administrator will not be able to directly open a connection from their PC to a domain controller, they always have to authenticate through the ManagementVMs first.

Domain Administrators

The domain administrator group is created per domain in the Active Directory forest. Accounts in this group have the second highest level of privilege, enterprise administrators have the highest level of privilege. Domain admin accounts should also only be used when absolutely necessary.

Note

The domain administrator group is not synced to the Azure AD cloud. Users have to be added to this group in the on-premise Active Directory.

Just like Enterprise Administrators, domain administrator accounts can connect to every machine in the domain over RDP or Remote PowerShell (WinRM). Following the security configurations which are explained in the installation manual, these connections can only be made when they are initiated from the ManagementVMs. The domain administrator will thus have to make the connections through the Windows Admin Center interface, which can be opened on any client computer.

This interface can be opened in a browser window on any client computer in the environment, the domain admin should log onto this client computer with a regular user account. The Windows Admin Center (WAC) interface can be opened by typing in the url, which should be the fully qualified domain name of the server on which WAC is being hosted. If WAC is being hosted on multiple servers which form a cluster, then this url will use the cluster hostname. This interface will present a login screen, in which the domain admin should log in to with an account with domain administrator privileges.

In Windows Admin Center the administrator can connect to all the servers and machines of the environment. To make AD domain configurations the administrator can use the Remote PowerShell or Remote Desktop Protocol option on the domain controllers, which will open a connection to manage the domain controller.

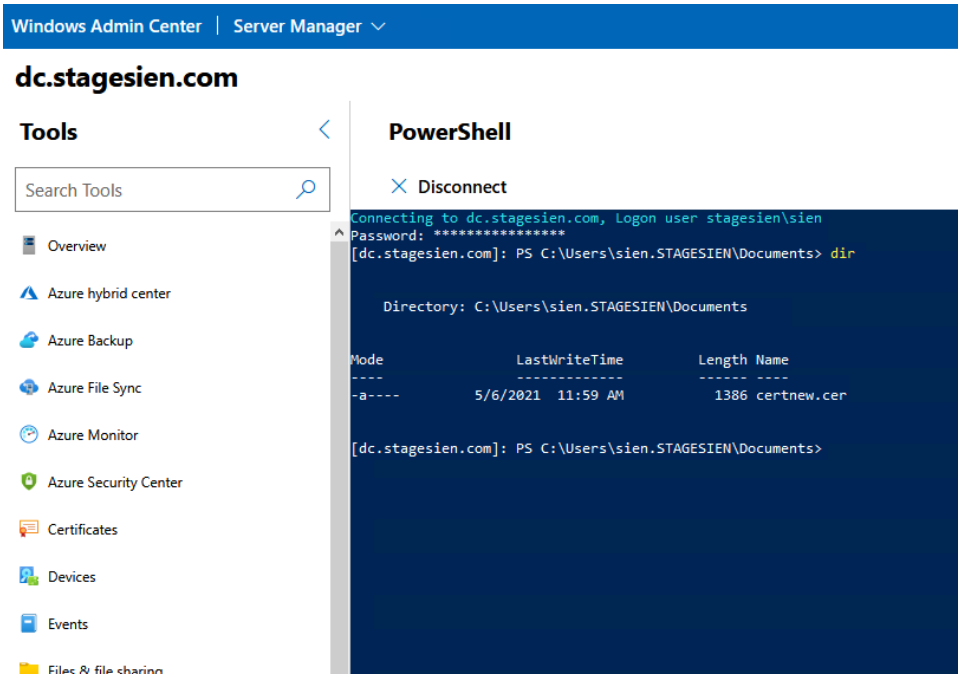

Figure 8: Remote PowerShell on a target through Windows Admin Center

Global Administrators

Global administrators have access to all administrative features in Azure Active Directory, as well as services that use Azure Active Directory identities like Microsoft 365 security center, Microsoft 365 compliance center, Exchange Online, SharePoint Online, and Skype for Business Online. The global administrator role is the role with the highest privileges in Azure Active Directory. The person who signs up for the Azure AD organization, gets registered as a global administrator.

Because of the high level of privileges, global administrator accounts should be monitored and secured properly. The amount of accounts with global administrative privileged should be limited to the necessary minimum.

Global administrator accounts have access to features, services, and settings which other accounts will not have access to. An example is Azure AD Connect Health.

Azure AD Connect Health is a solution that monitors the health of the Azure AD Connect Sync service. If an error occurs in this sync service, then data may not be properly synced between the on-premise and cloud environment. It is important to properly monitor this service using the Azure AD Connect Health tool to fix any issues before they can cause any damage. The interface of the Azure AD Connect Health tool can be found here. This portal can only be accessed by global administrators.

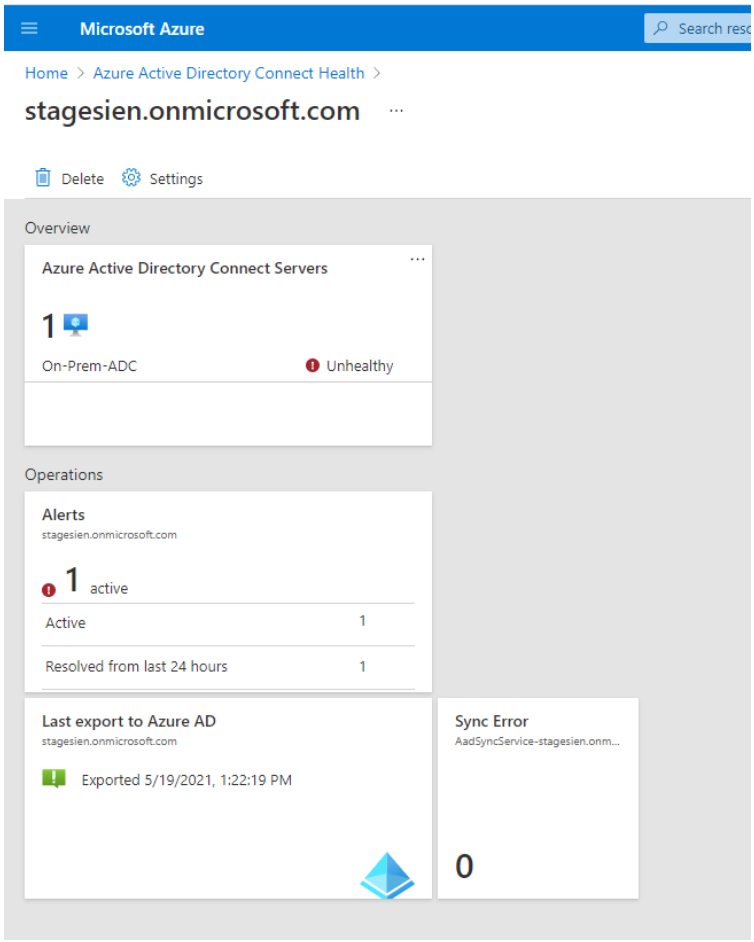

Figure 9: Azure AD Connect Health interface

A full overview of all the permissions a global administrator account has, can be found here.

Application Administrators

Application administrators are cloud (Azure AD) administrators that can manage and configure enterprise applications and app registrations in the Active Directory tenant. When an application gets registered in the Azure AD tenant, application administrators can configure the settings for this application and give users access to the application.

Windows Admin Center is an administrative tool that is registered when following the installation manual. After this registration, users with the application administrator role will be able to customize the settings of the application through the Azure AD portal. They can for example configure user access to the app.

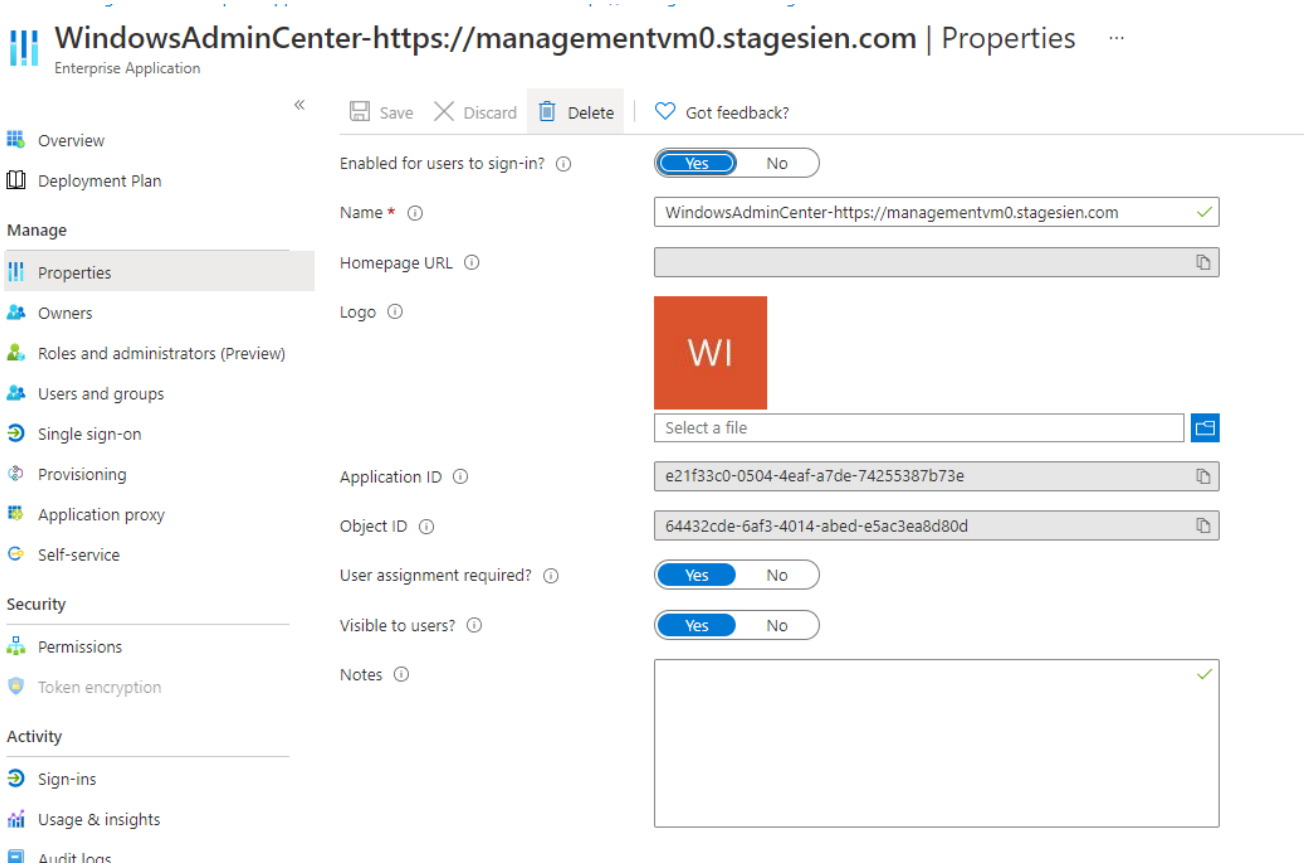

Figure 10: Windows Admin Center application in Azure AD

Every organization will host different applications and offer different services to their clients; these applications can all be managed by Application administrators after they have been registered in the Azure portal.

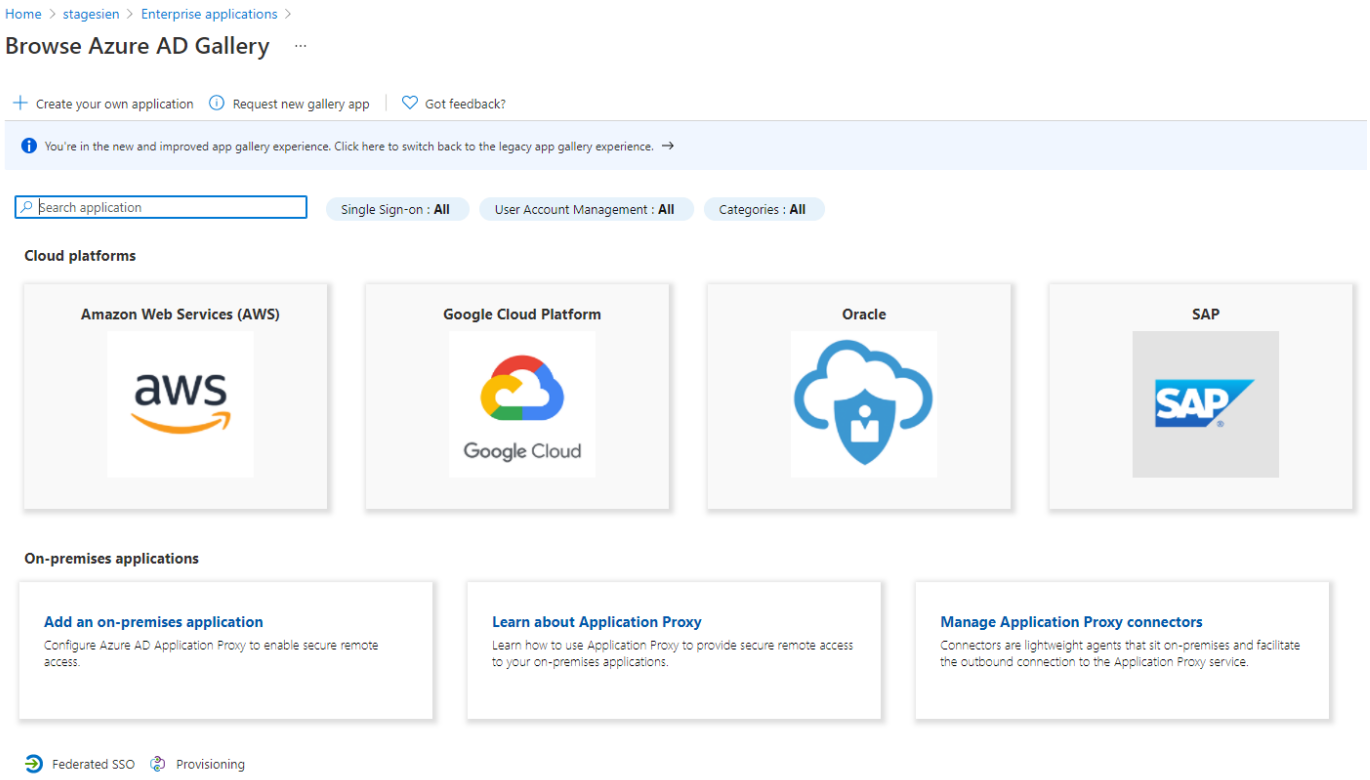

Figure 11: Registering a new application in Azure AD

3. Security operators

Like the name suggests, security operators are users that have privileges to use and configure security- and monitoring tools. There are a few different security and monitoring tools in the Hybrid IT management framework, such as Azure Monitor, Azure Log Analytics, and Azure Sentinel. Security Operators will have access to Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management and Office 365 Security & Compliance Center by default. Access to other services and tools will have to be configured by adding the role in Role Based Access Control per service/tool.

Azure Sentinel is a very advanced and customizable tool in the Hybrid IT Management framework. It has the possibility to visualize data, create alerts and incidents, create automated responses to alerts/incidents, and deep dive in incidents to discover the causes. This is a great tool if utilized properly.

The installation manual describes how workbooks can be created to visualize data, how alerts and incident creation rules can be configured, and how automated responses (playbooks) can be created by providing some examples. These examples can be used by building on them to create custom workbooks, incidents, and playbooks. Which can then be used by security operators to monitor and secure the entire environment.

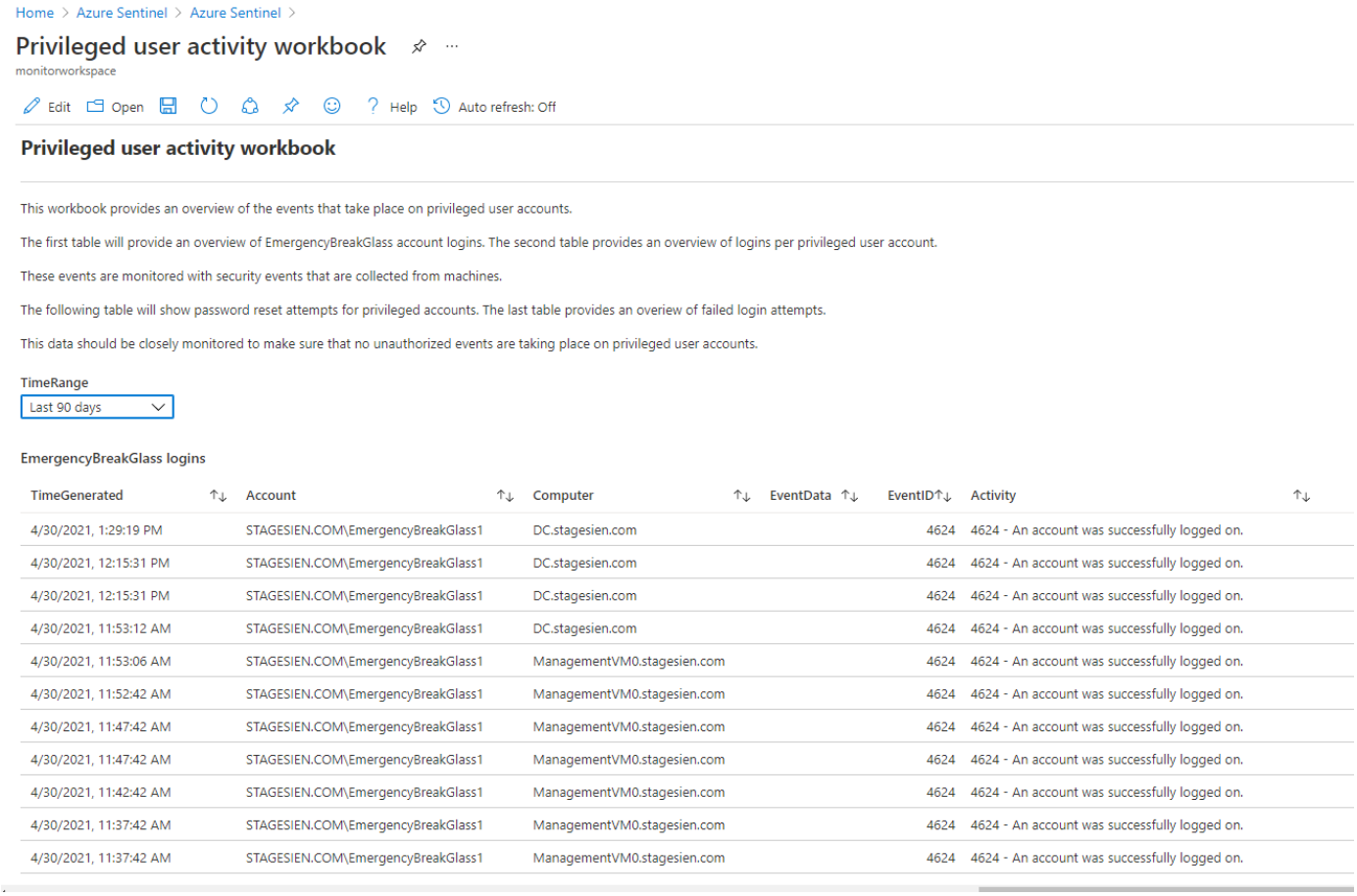

Figure 12: Example of a workbook in Azure Sentinel

Queries can be tested in a log analytics workspace before being implemented in a workbook or incident creation rule. This Microsoft Docs page provides a tutorial on how to create custom workbooks.

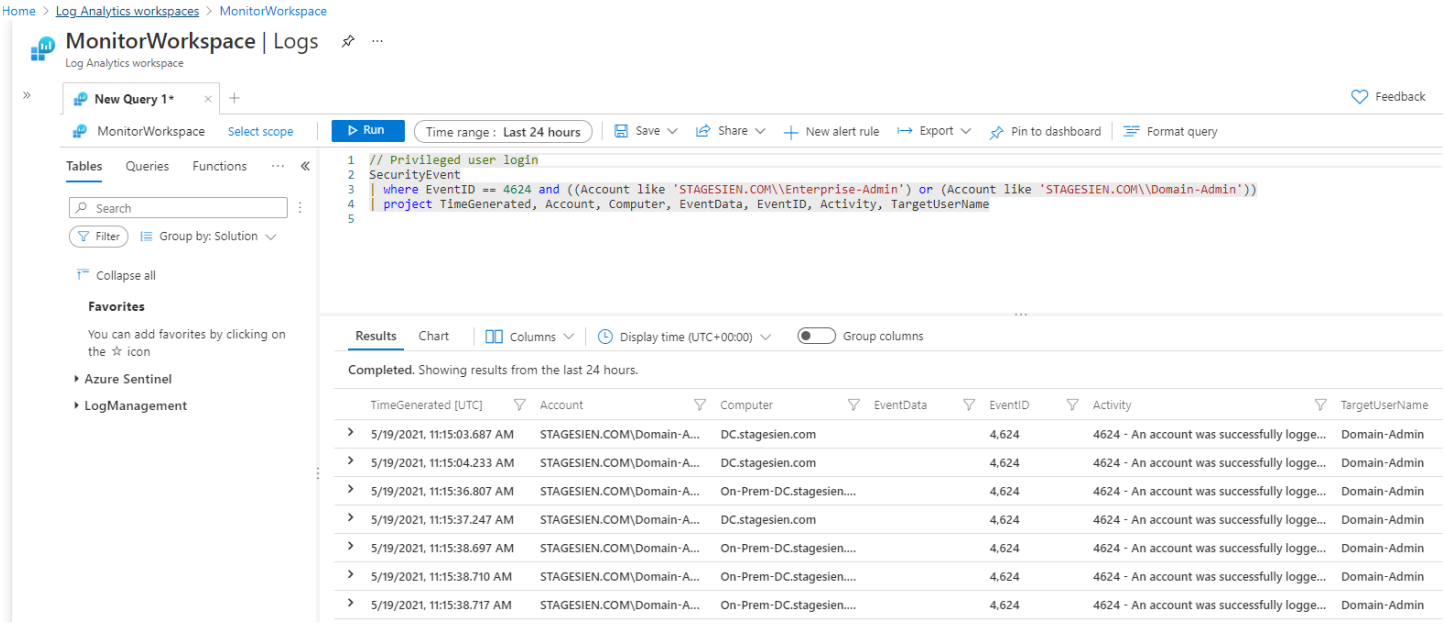

Figure 13: Example of a query in an Azure log analytics workspace

Documentation on how to create custom queries can be found on this Microsoft Docs page.

When an incident is triggered it will appear in the Incidents tab in Azure Sentinel. Incident creation rules can be configured using the same queries that are used in Azure Monitor and azure Log Analytics workspaces. More information about incident creation rules can be found here.

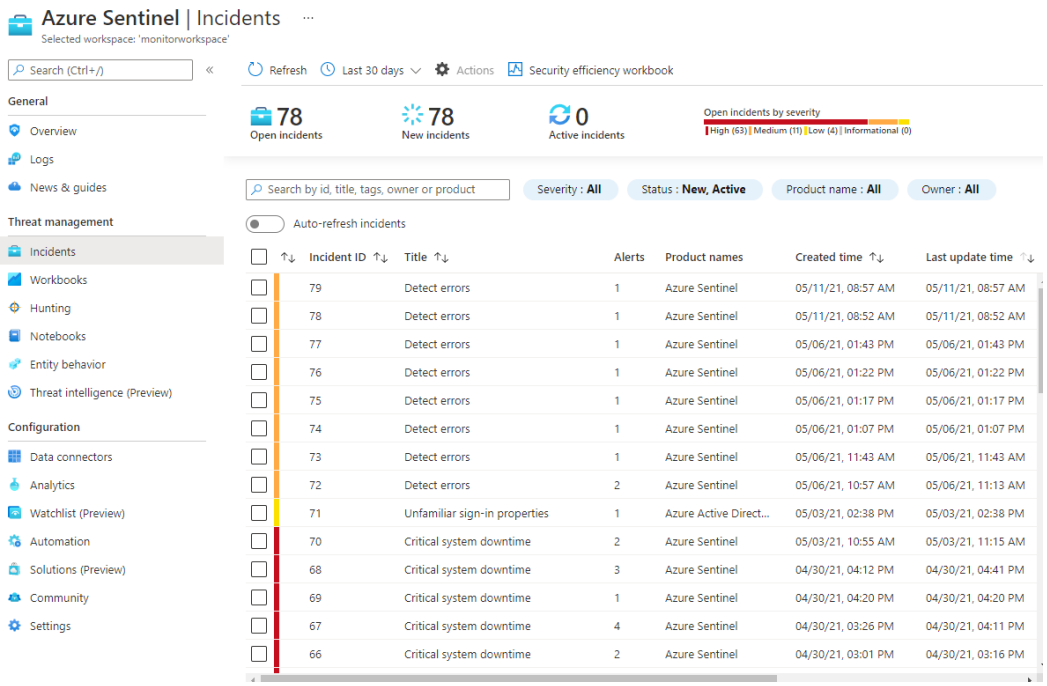

Figure 14: Azure Sentinel Incidents