

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

Document Revision History2

Introduction4

1. Users5

2. Administrators7

 Enterprise Administrator.....8

 Domain Administrators.....10

 Global Administrators.....11

 Application Administrators.....12

3. Security operators14

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.

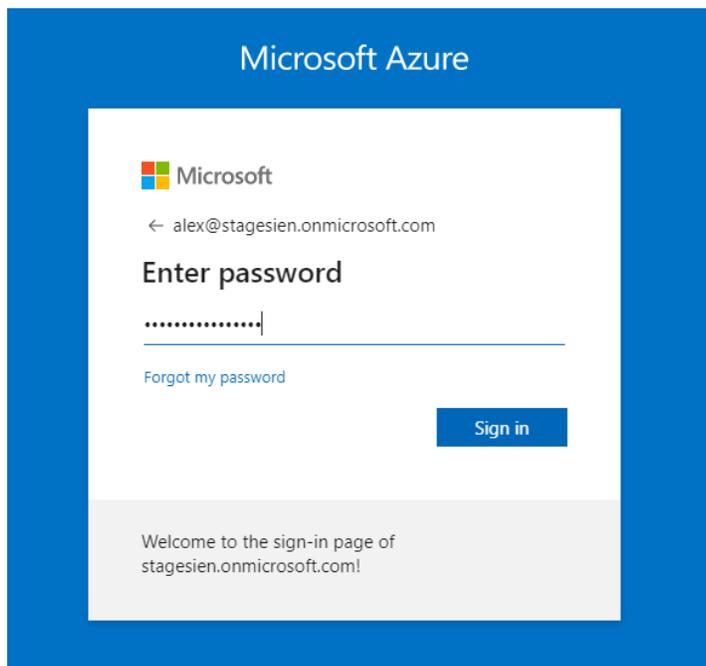


Figure 1: Microsoft Azure login screen

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.



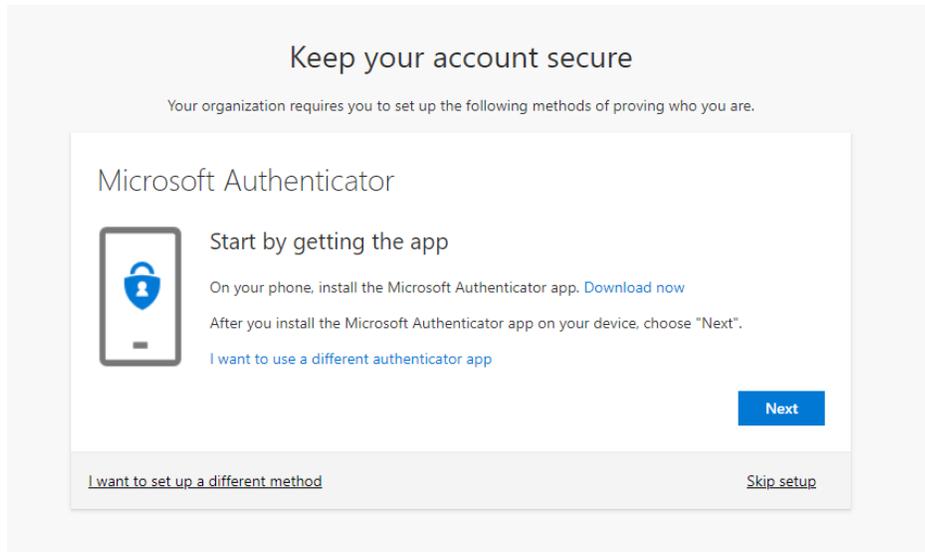


Figure 2: Multiple Factor Authentication

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.

Microsoft

Get back into your account

Who are you?

To recover your account, begin by entering your email or username and the characters in the picture or audio below.

Email or Username:

Example: user@contoso.onmicrosoft.com or user@contoso.com



Enter the characters in the picture or the words in the audio.

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.

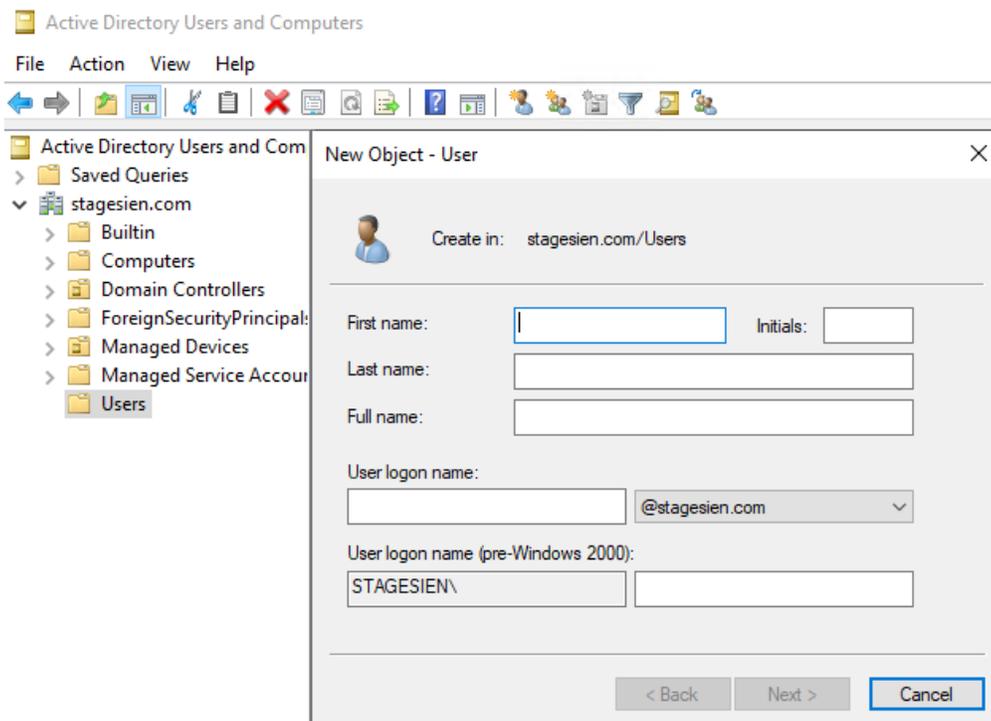


Figure 4: New Active Directory administrator account



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.

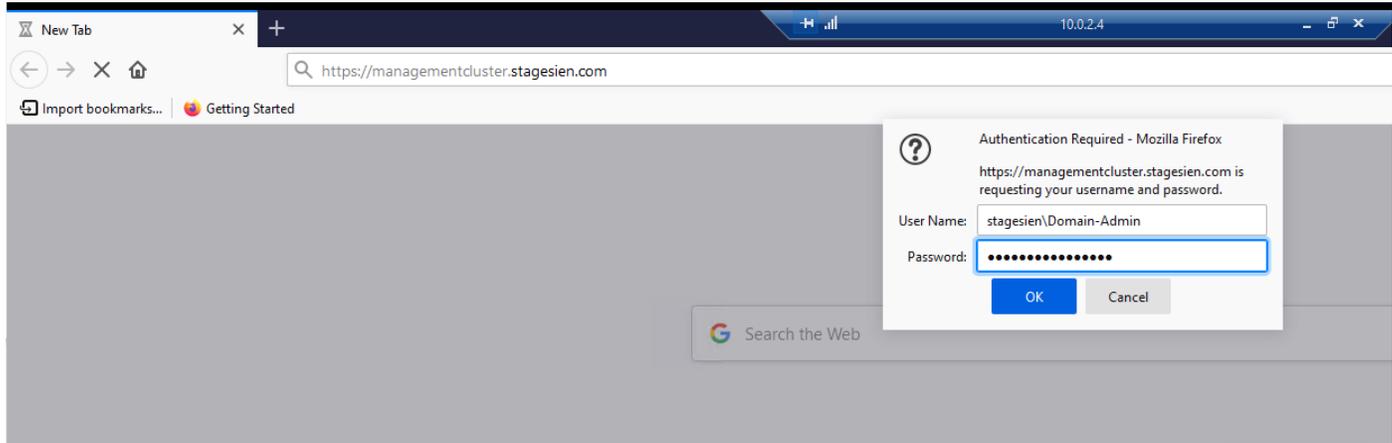


Figure 6: Windows Admin Center login screen

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.

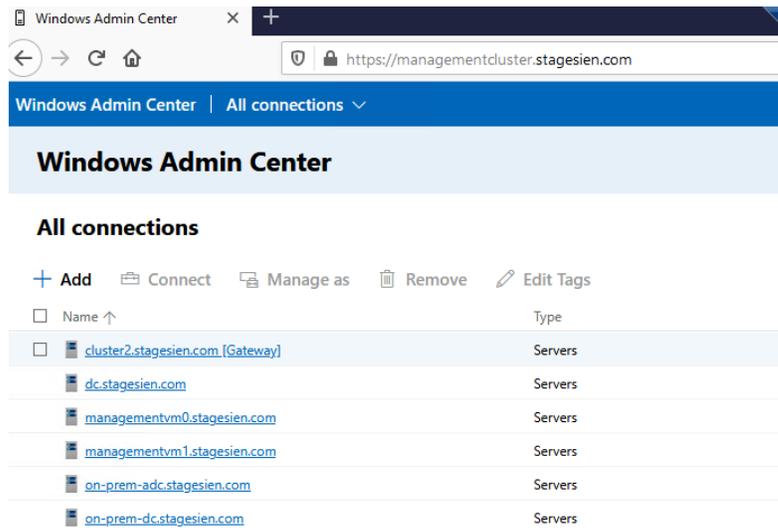


Figure 7: Windows Admin Center interface

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.

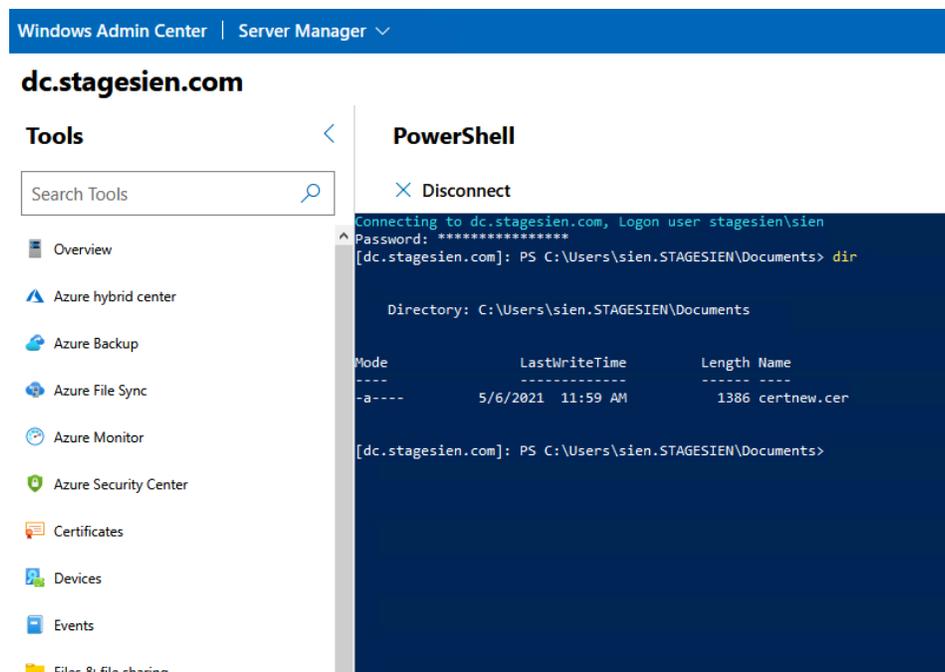


Figure 8: Remote PowerShell on a target through Windows Admin Center



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.

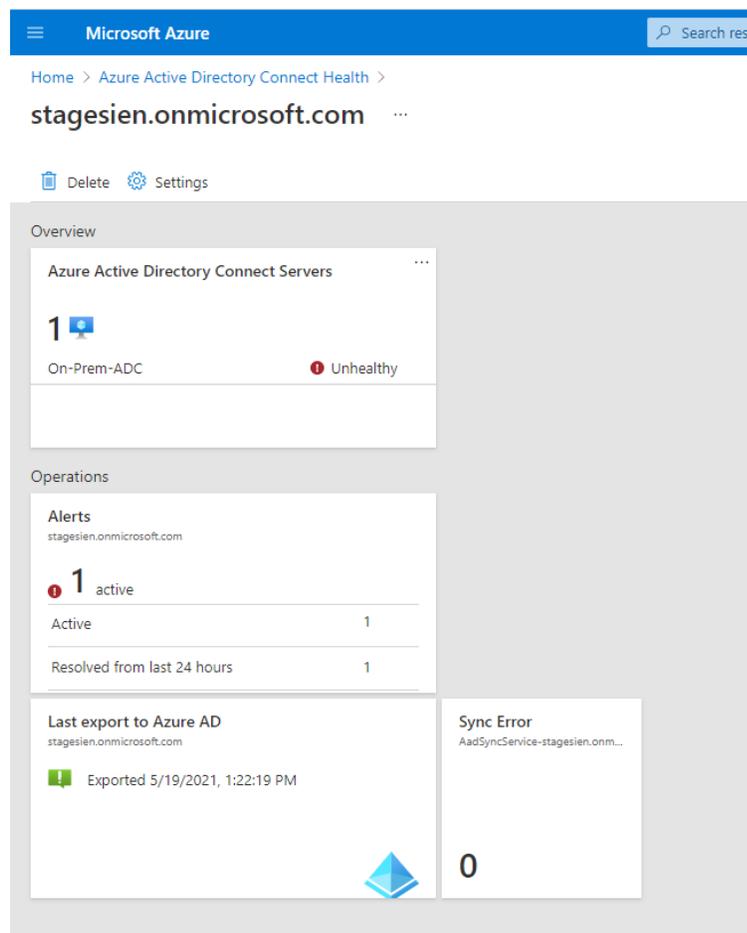


Figure 9: Azure AD Connect Health interface

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.

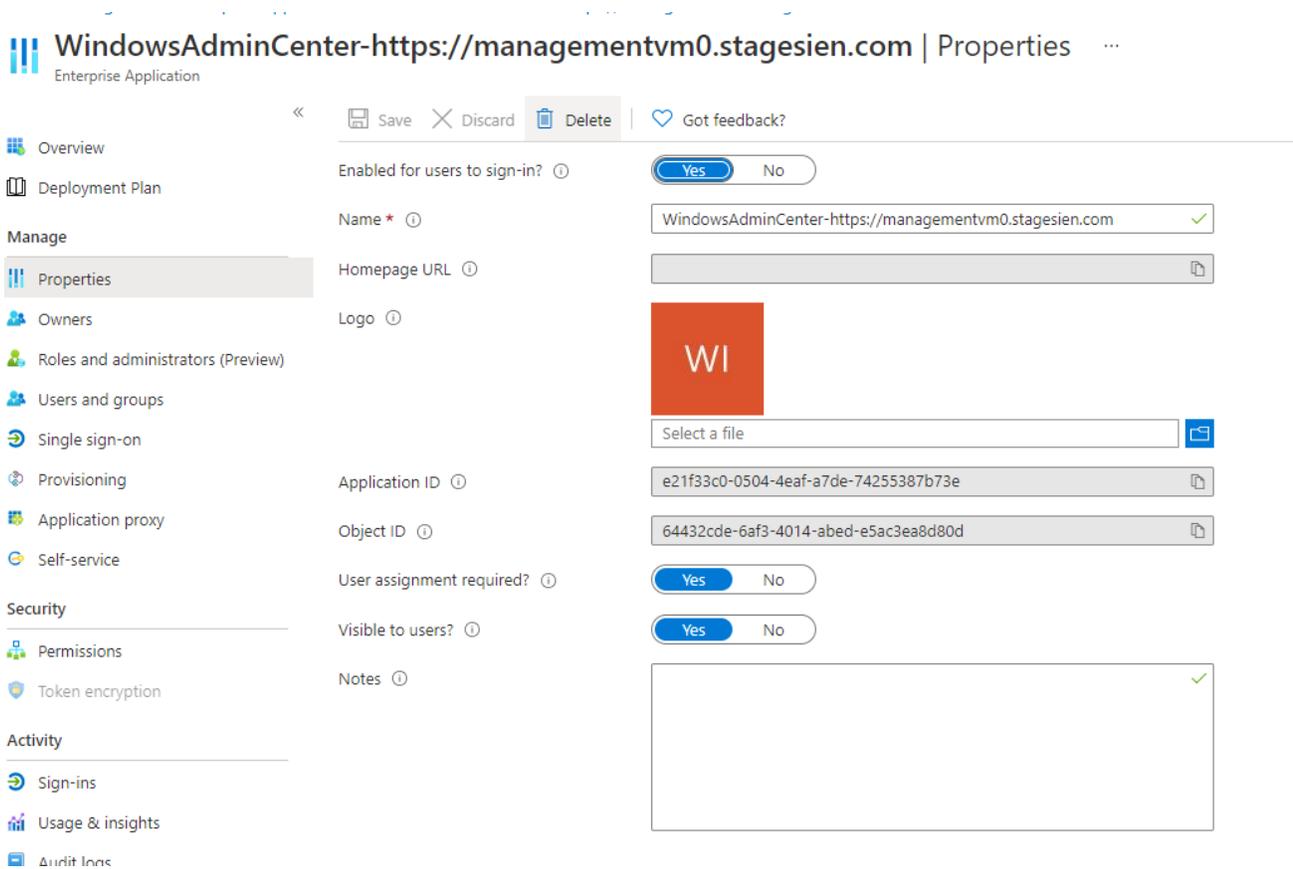


Figure 10: Windows Admin Center application in Azure AD

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.



Home > stagesien > Enterprise applications >

Browse Azure AD Gallery

+ Create your own application | Request new gallery app | Got feedback?

You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

Search application

Single Sign-on : All

User Account Management : All

Categories : All

Cloud platforms

The 'Cloud platforms' section displays four application cards. Each card features a logo and the name of the platform: Amazon Web Services (AWS), Google Cloud Platform, Oracle, and SAP.

On-premises applications

The 'On-premises applications' section contains three cards. The first card is titled 'Add an on-premises application' and describes configuring Azure AD Application Proxy for secure remote access. The second card is titled 'Learn about Application Proxy' and explains how to use the service for secure remote access. The third card is titled 'Manage Application Proxy connectors' and describes the role of connectors as lightweight agents for outbound connections.

Federated SSO | Provisioning

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.

Home > Azure Sentinel > Azure Sentinel >

Privileged user activity workbook

monitorworkspace

Edit Open Refresh Save Help Auto refresh: Off

Privileged user activity workbook

This workbook provides an overview of the events that take place on privileged user accounts.

The first table will provide an overview of EmergencyBreakGlass account logins. The second table provides an overview of logins per privileged user account.

These events are monitored with security events that are collected from machines.

The following table will show password reset attempts for privileged accounts. The last table provides an overview of failed login attempts.

This data should be closely monitored to make sure that no unauthorized events are taking place on privileged user accounts.

TimeRange

Last 90 days

EmergencyBreakGlass logins

TimeGenerated	Account	Computer	EventData	EventID	Activity
4/30/2021, 1:29:19 PM	STAGESIEN.COM\EmergencyBreakGlass1	DC.stagesien.com		4624	4624 - An account was successfully logged on.
4/30/2021, 12:15:31 PM	STAGESIEN.COM\EmergencyBreakGlass1	DC.stagesien.com		4624	4624 - An account was successfully logged on.
4/30/2021, 12:15:31 PM	STAGESIEN.COM\EmergencyBreakGlass1	DC.stagesien.com		4624	4624 - An account was successfully logged on.
4/30/2021, 11:53:12 AM	STAGESIEN.COM\EmergencyBreakGlass1	DC.stagesien.com		4624	4624 - An account was successfully logged on.
4/30/2021, 11:53:06 AM	STAGESIEN.COM\EmergencyBreakGlass1	ManagementVM0.stagesien.com		4624	4624 - An account was successfully logged on.
4/30/2021, 11:52:42 AM	STAGESIEN.COM\EmergencyBreakGlass1	ManagementVM0.stagesien.com		4624	4624 - An account was successfully logged on.
4/30/2021, 11:47:42 AM	STAGESIEN.COM\EmergencyBreakGlass1	ManagementVM0.stagesien.com		4624	4624 - An account was successfully logged on.
4/30/2021, 11:47:42 AM	STAGESIEN.COM\EmergencyBreakGlass1	ManagementVM0.stagesien.com		4624	4624 - An account was successfully logged on.
4/30/2021, 11:42:42 AM	STAGESIEN.COM\EmergencyBreakGlass1	ManagementVM0.stagesien.com		4624	4624 - An account was successfully logged on.
4/30/2021, 11:37:42 AM	STAGESIEN.COM\EmergencyBreakGlass1	ManagementVM0.stagesien.com		4624	4624 - An account was successfully logged on.
4/30/2021, 11:37:42 AM	STAGESIEN.COM\EmergencyBreakGlass1	ManagementVM0.stagesien.com		4624	4624 - An account was successfully logged on.

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.



The screenshot shows the Azure Log Analytics workspace interface. At the top, there's a navigation bar with 'Home > Log Analytics workspaces > MonitorWorkspace'. Below that, the workspace name 'MonitorWorkspace | Logs' is displayed. A query editor on the left shows a query for 'Privileged user login' with the following KQL code:

```
1 // Privileged user login
2 SecurityEvent
3 | where EventID == 4624 and ((Account like 'STAGESIEN.COM\\Enterprise-Admin') or (Account like 'STAGESIEN.COM\\Domain-Admin'))
4 | project TimeGenerated, Account, Computer, EventData, EventID, Activity, TargetUserName
5
```

The results table below the query shows the following data:

TimeGenerated [UTC]	Account	Computer	EventData	EventID	Activity	TargetUserName
5/19/2021, 11:15:03.687 AM	STAGESIEN.COM\Domain-A...	DC.stagesien.com		4624	4624 - An account was successfully logge...	Domain-Admin
5/19/2021, 11:15:04.233 AM	STAGESIEN.COM\Domain-A...	DC.stagesien.com		4624	4624 - An account was successfully logge...	Domain-Admin
5/19/2021, 11:15:36.807 AM	STAGESIEN.COM\Domain-A...	On-Prem-DC.stagesien....		4624	4624 - An account was successfully logge...	Domain-Admin
5/19/2021, 11:15:37.247 AM	STAGESIEN.COM\Domain-A...	DC.stagesien.com		4624	4624 - An account was successfully logge...	Domain-Admin
5/19/2021, 11:15:38.697 AM	STAGESIEN.COM\Domain-A...	On-Prem-DC.stagesien....		4624	4624 - An account was successfully logge...	Domain-Admin
5/19/2021, 11:15:38.710 AM	STAGESIEN.COM\Domain-A...	On-Prem-DC.stagesien....		4624	4624 - An account was successfully logge...	Domain-Admin
5/19/2021, 11:15:38.717 AM	STAGESIEN.COM\Domain-A...	On-Prem-DC.stagesien....		4624	4624 - An account was successfully logge...	Domain-Admin

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](#).

The screenshot shows the Azure Sentinel Incidents page. At the top, there's a navigation bar with 'Azure Sentinel | Incidents'. Below that, there's a summary section with '78 Open incidents', '78 New incidents', and '0 Active incidents'. A bar chart shows 'Open incidents by severity' with 'High (63)', 'Medium (1)', and 'Low (4) Informational (9)'. Below the summary, there's a search bar and filters for 'Severity: All', 'Status: New, Active', 'Product name: All', and 'Owner: All'. The main table lists incidents with columns for Incident ID, Title, Alerts, Product names, Created time, and Last update time.

Incident ID	Title	Alerts	Product names	Created time	Last update time
79	Detect errors	1	Azure Sentinel	05/11/21, 08:57 AM	05/11/21, 08:57 AM
78	Detect errors	1	Azure Sentinel	05/11/21, 08:52 AM	05/11/21, 08:52 AM
77	Detect errors	1	Azure Sentinel	05/06/21, 01:43 PM	05/06/21, 01:43 PM
76	Detect errors	1	Azure Sentinel	05/06/21, 01:22 PM	05/06/21, 01:22 PM
75	Detect errors	1	Azure Sentinel	05/06/21, 01:17 PM	05/06/21, 01:17 PM
74	Detect errors	1	Azure Sentinel	05/06/21, 01:07 PM	05/06/21, 01:07 PM
73	Detect errors	1	Azure Sentinel	05/06/21, 11:43 AM	05/06/21, 11:43 AM
72	Detect errors	2	Azure Sentinel	05/06/21, 10:57 AM	05/06/21, 11:13 AM
71	Unfamiliar sign-in properties	1	Azure Active Direct...	05/03/21, 02:38 PM	05/03/21, 02:38 PM
70	Critical system downtime	2	Azure Sentinel	05/03/21, 10:55 AM	05/03/21, 11:15 AM
68	Critical system downtime	3	Azure Sentinel	04/30/21, 04:12 PM	04/30/21, 04:41 PM
69	Critical system downtime	1	Azure Sentinel	04/30/21, 04:20 PM	04/30/21, 04:20 PM
67	Critical system downtime	4	Azure Sentinel	04/30/21, 03:26 PM	04/30/21, 04:11 PM
66	Critical system downtime	2	Azure Sentinel	04/30/21, 03:01 PM	04/30/21, 03:16 PM

Figure 14: Azure Sentinel Incidents

