

Modern Workplace with Secure Score v2.1

Click-to-Run™ Deployment Guide



Modern Workplace with Secure Score

Deployment Guide

This guide was designed to provide channel partners with the post deployment steps required to successfully deploy Azure Secure Score v2.1.

Below is a list of action items as part of the deployment process and post deployment recommendations to customize the cloud environment.

Content

Technical Requirements

Required features for deploy specific features of the solution.

- Azure Active Directory License
- Azure 365 License

Deployment

Extended information about each available features.

- Previous Versions
- Deployment Type
- Automation Account
- User Security
- 365 Security
- Advanced Options

Post Deployment

How to modify deployed configurations steps after deployment.

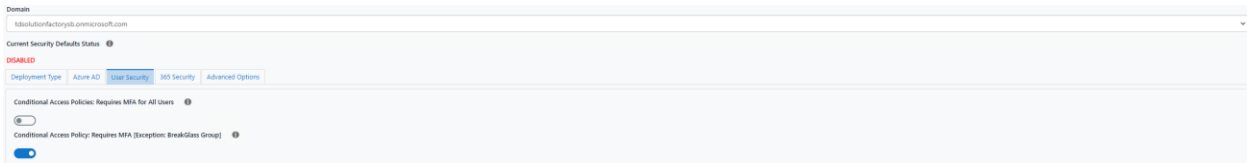
- Resource Group
- Automation Account
- Runbooks
- Runbook Monitoring
- Troubleshooting

Technical Requirements

Azure Active Directory License

Conditional Access Features could change depending of the Azure AD License available. The solution will check if at least 1 user has Premium license assigned (P1 or P2). Depending of the License Conditional Access Policies will remain blocked:

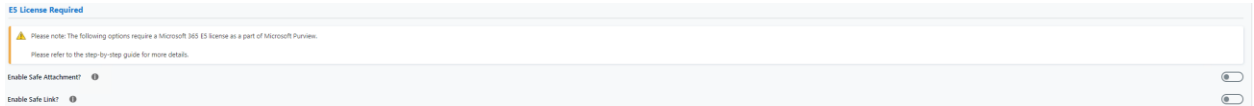
- License non Premium (AAD Free or 365)
 - Conditional Access Policies: Unavailable
 - Security Defaults: Required
- License Premium (AAD P1 or AAD P2)
 - Conditional Access Policies: Available (if Security Defaults is Disabled)
 - Security Defaults: Available



Azure 365 License

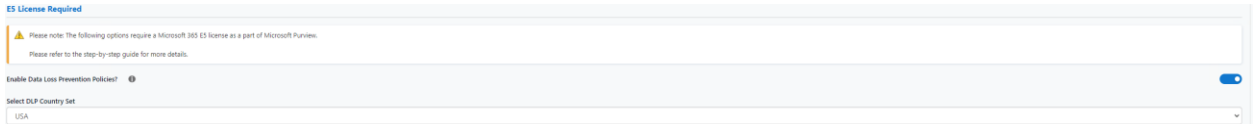
365 Security Features could not be available if 365 Premium License is not available (E5 license). Depending of the License Security Features will not be available:

- 365 Security Functions:



The screenshot shows a configuration page for 365 Security Functions. At the top, there is a blue header that reads "E5 License Required". Below this, a yellow warning triangle icon is followed by the text: "Please note: The following options require a Microsoft 365 E5 license as a part of Microsoft Purview. Please refer to the step-by-step guide for more details." Below the warning, there are two toggle switches. The first is labeled "Enable Safe Attachment?" and is currently turned off. The second is labeled "Enable Safe Link?" and is also currently turned off.

- 365 Data Loss Prevention:



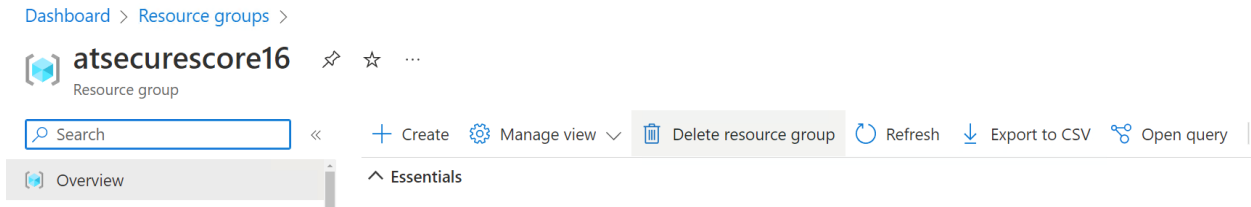
The screenshot shows a configuration page for 365 Data Loss Prevention. At the top, there is a blue header that reads "E5 License Required". Below this, a yellow warning triangle icon is followed by the text: "Please note: The following options require a Microsoft 365 E5 license as a part of Microsoft Purview. Please refer to the step-by-step guide for more details." Below the warning, there is a toggle switch labeled "Enable Data Loss Prevention Policies?" which is currently turned on. Below the toggle, there is a dropdown menu labeled "Select DLP Country Set" with "USA" selected.

Deployment

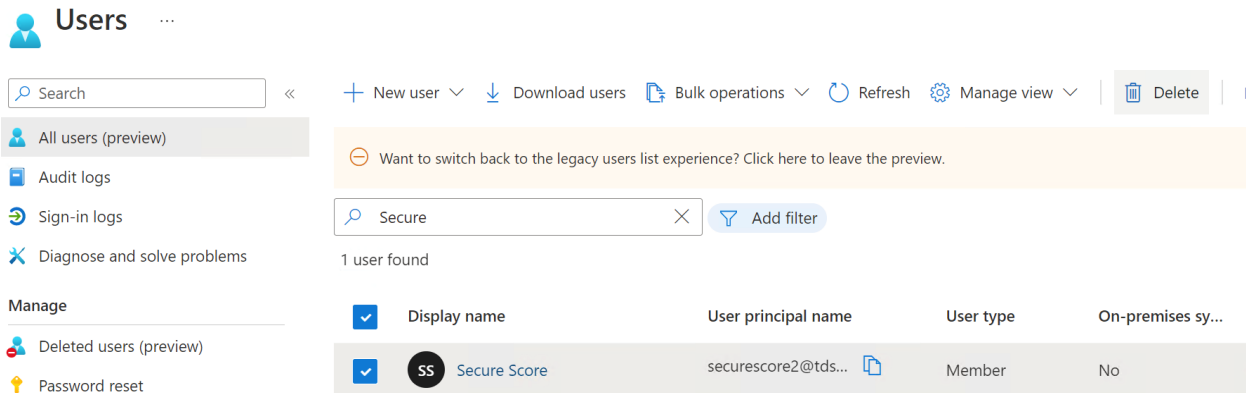
Previous Versions

Previous Versions of Secure Scores can't create any conflict on version 2.1, however, our recommendation is removing old versions before proceed. To remove old versions, go to:

- Resource Group:
 - o Go to Secure Score Resource Group.
 - o Click on **“Delete resource group”** to delete all the objects.



- Secure Score User:
 - o Go to Azure AD.
 - o Click on Users.
 - o Search for Secure Score User.
 - o Click on **“Delete”**.



Deployment Type

Deployment Type depends of the type of license available on Azure AD, if License is a P1 or P2 both options can be deployed: Conditional Access Policies or Security Defaults.

In case AAD License is free only Security Defaults is available.

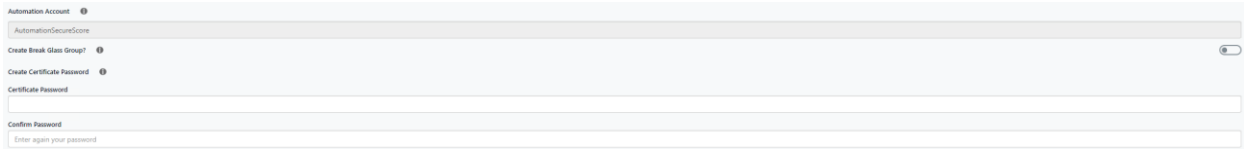


- **Secure Score without Security Defaults: Conditional Access Policies available to deploy.**
 - Conditional Access Policies will:
 - MFA Enforcement for all users.
 - MFA Enforcement for all users with exception.

- **Secure Score with Security Defaults: Only Security Defaults could be use as MFA tool.**
 - Security Defaults will:
 - MFA Enforcement for all users.
 - Legacy Auth Denied for all apps.

Azure AD

Azure AD section will allow us to create exception group for MFA, Certificate password for authentication account “AutomationSecureScorerunAs”.



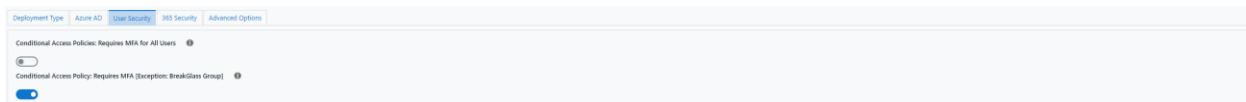
- Automation Account: Automation account Name for manage and deploy configurations on 365 and Data Compliance Center. “AutomationSecureScore” will be assigned as Exchange Administrator (365 email parameters) and Data Compliance Administrator (Data Loss Prevention Policies).
- BreakGlass Group: Create an Azure AD Group for Accounts that should bypass MFA enforcement.
- Certificate Password: Automation Account will be validated using a Certificate managed by Azure AD. This password will be used to sign certificate and allow exportation. **Please note:** We recommend to store certificate password in a secure place

Certificate Default Expiration Date: 1 year.

User Security

If Deployment Type is set as “Secure Score without Security Defaults” this section will allow us to choose which Conditional Access Policy we want to deploy in our tenant. **Please note:** A license P1 or P2 is required to deploy Conditional Access Policies.

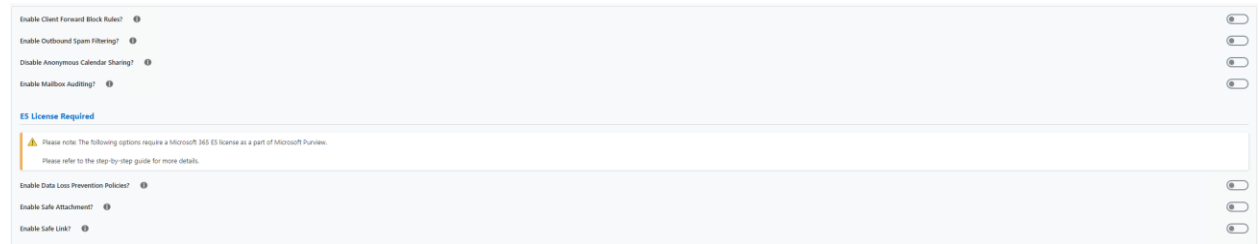
Deployment without Security Defaults



- MFA : Require MFA for all Users, will enforce MFA for all users with a grace period of 14 days to allow users to set MFA devices (Microsoft Authenticator or Phone number).
- MFA with Exception: MFA for all Users, BUT an exception will be created for AAD Group “**Break Glass**”.

365 Security

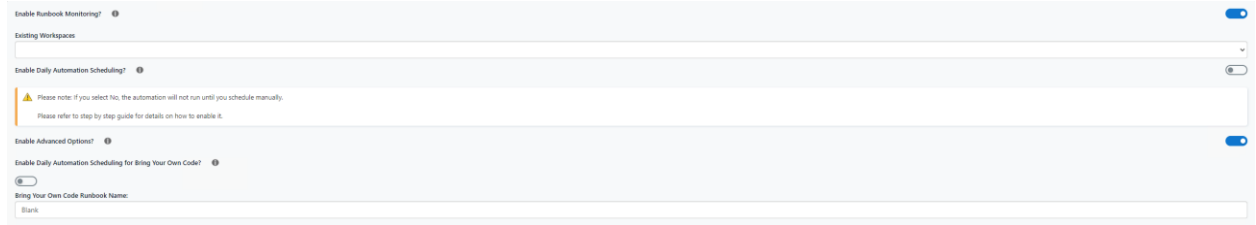
365 Security is a set of security features to deploy on 365 Configuration and Data Compliance Center (Data Loss Prevention), all these features can be enabled/disabled after deployment by Runbooks variable configuration. **Please note:** A license E5 is required to deploy Data Loss Policies.



- **Client Forward Block:** Allows security control to create a transport rule to stop external, auto-forward type messages from leaving your tenant.
- **Outbound Spam Filter:** Allows the challenge of IP block listing that occurs when your network is blocked because spammers have managed to infiltrate it and use it to send spam.
- **Anonymous Calendar Share:** By default, sharing is enabled, as an Office 365 admin can you decide what kind of information your user share externally. With Anonymous calendar sharing enabled the following can be set.
- **Mailbox Audit:** Allows you to track actions that users take within their own and other's mailboxes.
- **Data Loss Prevention:** Policies that are defined within Office 365 will govern data and send notifications when a rule is violated. The DLP feature in Office 365 will automatically classify data and use the set policies to stop an email from being sent and block unauthorized access to classified content.
- **Safe Attachment:** A feature of Microsoft 365 Advanced Threat Protection. When configured, it protects users from compromised attachments.
- **Safe Link:** A feature of Defender for Office 365 that provides URL scanning and rewriting of inbound email messages in mail flow, and time-of-click verification of URLs and links in email messages and other locations.

Advanced Options

In addition, some extra configurations can be done to allow monitoring and automation execution of runbooks, also you can Upload your own code to execute automatically. **Please note:** Monitoring with Workspace will require some manual steps.

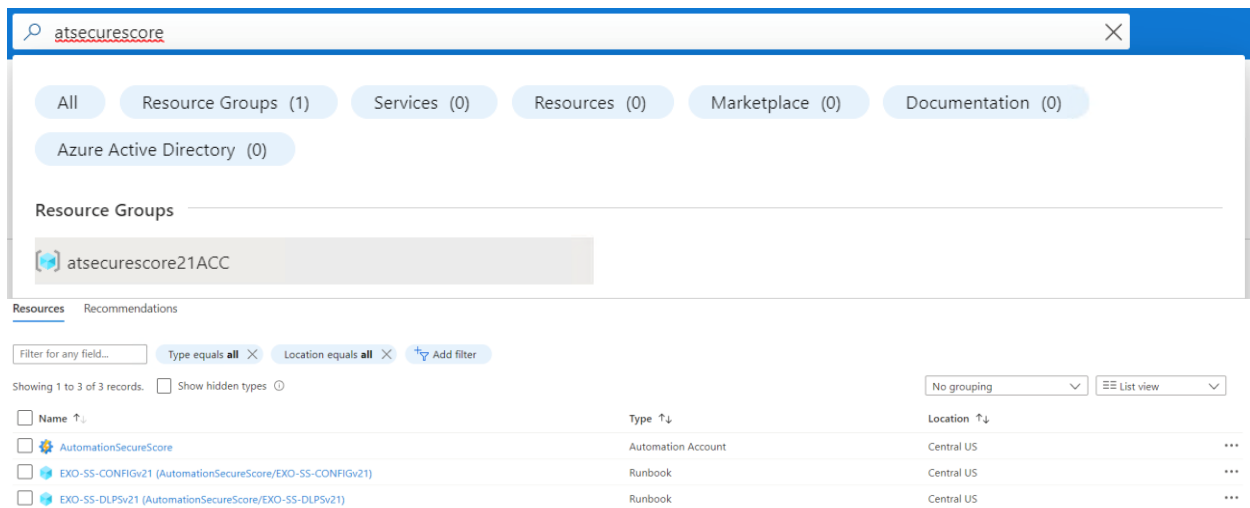


- Runbook Monitor: Allows to track Runbooks execution and results, if enabled an existing Analytics workspace will be required to connect automation account.
- Daily Automation Scheduling: Allows to automatically run, runbooks to check and reapply email configuration.
- Daily Automation Scheduling for BYOC: Allows to automatically run our own runbooks.
- Bring Your Own Code: Allows to upload our own runbooks.

Post Deployment

Resource Group

After Deployment all our resources can be found on the selected Resource Group. To find your new Solution, write resource group name on Search tab.

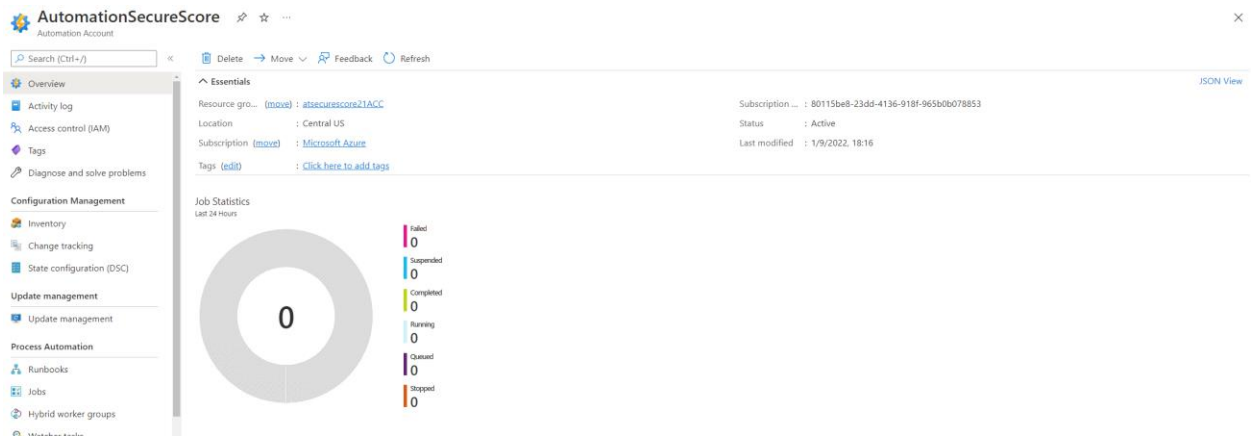


The screenshot shows the Azure portal search interface. The search bar contains 'atsecurescore'. Below the search bar, there are tabs for 'All', 'Resource Groups (1)', 'Services (0)', 'Resources (0)', 'Marketplace (0)', and 'Documentation (0)'. Under the 'Resource Groups' section, a single result 'atsecurescore21ACC' is displayed. Below this, there are tabs for 'Resources' and 'Recommendations'. The 'Resources' tab is active, showing a list of resources with filters for 'Type equals all' and 'Location equals all'. The list shows 3 records:

| Name | Type | Location |
|---|--------------------|------------|
| AutomationSecureScore | Automation Account | Central US |
| EXO-SS-CONFIGv21 (AutomationSecureScore/EXO-SS-CONFIGv21) | Runbook | Central US |
| EXO-SS-DLPsv21 (AutomationSecureScore/EXO-SS-DLPsv21) | Runbook | Central US |

Automation Account

Azure Policies Features Azure Policy uses a JSON format to form the logic the evaluation uses to determine whether a resource is compliant or not. Definitions include metadata and the policy rule. The defined rule can use functions, parameters, logical operators, conditions, and property aliases to match exactly the scenario you want. The policy rule determines which resources in the scope of the assignment get evaluated and blocked or allowed depending on the statement.



- Modify Variables:

+ Add a variable Refresh

Search variables...

| Name | Type | Value | Last modified |
|---------------------------------------|--------|---------------------|-----------------|
| AnonymousCalendarSharingRules_Enabled | String | false | 1/9/2022, 18:18 |
| BYOC_Runbook_Name | String | Blank | 1/9/2022, 18:18 |
| ClientForwardBlockRules_Enabled | String | false | 1/9/2022, 18:16 |
| DLPRules_DeploymentMode | String | AuditAndNotify | 1/9/2022, 18:18 |
| DLPRules_Enabled | String | false | 1/9/2022, 18:16 |
| DLPRules_Selection | String | USA | 1/9/2022, 18:16 |
| MailboxAuditingRules_Enabled | String | false | 1/9/2022, 18:18 |
| OutboundSpamFilteringRules_Enabled | String | false | 1/9/2022, 18:16 |
| SafeAttachmentRules_Enabled | String | false | 1/9/2022, 18:18 |
| SafeLinkRules_Enabled | String | false | 1/9/2022, 18:18 |
| SCM_Domain | String | tdsolutionfactorysb | 1/9/2022, 18:16 |

- Manage Certificate:

- Go to search bar and type “seurescorenew-runas”
- Click on “seurescorenew-runas” Application

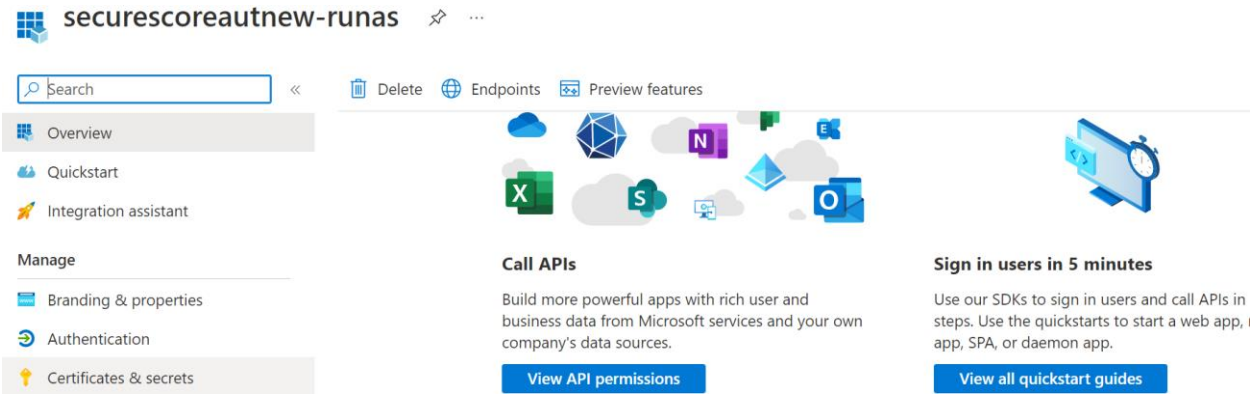
seurescoreautnew-runas

- All
- Azure Active Directory (2)
- Services (0)
- Resources (0)
- Resource Groups (0)
- Marketplace (0)
- Documentation (0)

Azure Active Directory

seurescoreautnew-runas Application seurescoreautnew-runas Service Principal

- On left bar search for **“Certificates & Secrets”**



seurescoreautnew-runas

Search

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets**

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

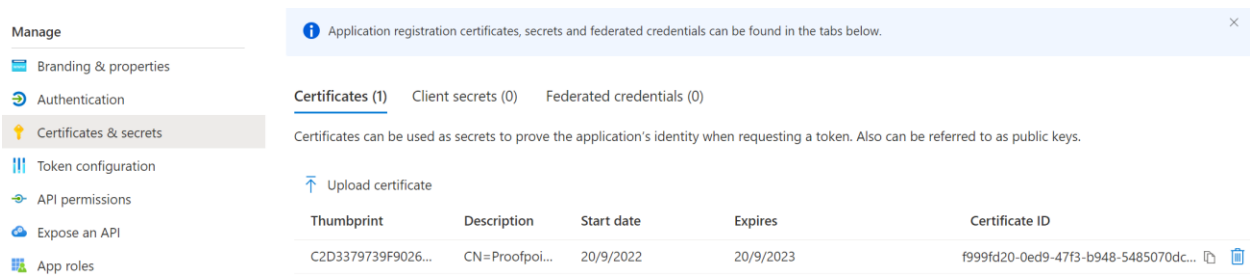
[View API permissions](#)

Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in steps. Use the quickstarts to start a web app, SPA, or daemon app.

[View all quickstart guides](#)

- On that section we will be able to remove Certificate or upload a new one.



Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (1) Client secrets (0) Federated credentials (0)

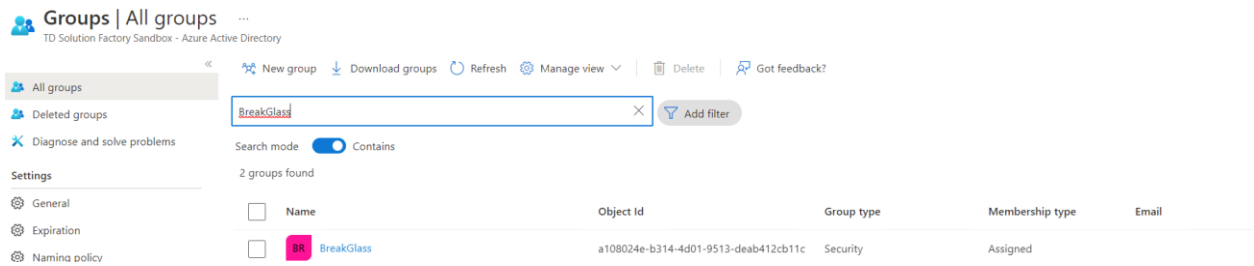
Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

| Thumbprint | Description | Start date | Expires | Certificate ID |
|--------------------|----------------|------------|-----------|--------------------------------------|
| C2D3379739F9026... | CN=Proofpoi... | 20/9/2022 | 20/9/2023 | f999fd20-0ed9-47f3-b948-5485070dc... |

Break Glass Group

Azure Policies Features Azure Policy uses a JSON format to form the logic the evaluation uses to determine whether a resource is compliant or not. Definitions include metadata and the policy rule. The defined rule can use functions, parameters, logical operators, conditions, and property aliases to match exactly the scenario you want. The policy rule determines which resources in the scope of the assignment get evaluated and blocked or allowed depending on the statement.



Groups | All groups ...
TD Solution Factory Sandbox - Azure Active Directory

New group Download groups Refresh Manage view Delete Got feedback?

All groups Deleted groups Diagnose and solve problems

Settings
General Expiration Naming policy

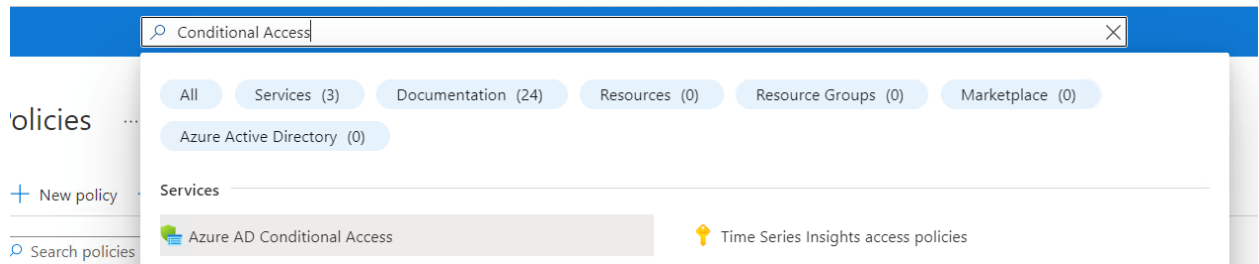
Search mode Contains
2 groups found

| <input type="checkbox"/> | Name | Object Id | Group type | Membership type | Email |
|--------------------------|----------------------|--------------------------------------|------------|-----------------|-------|
| <input type="checkbox"/> | BR BreakGlass | a108024e-b314-4d01-9513-deab412cb11c | Security | Assigned | |

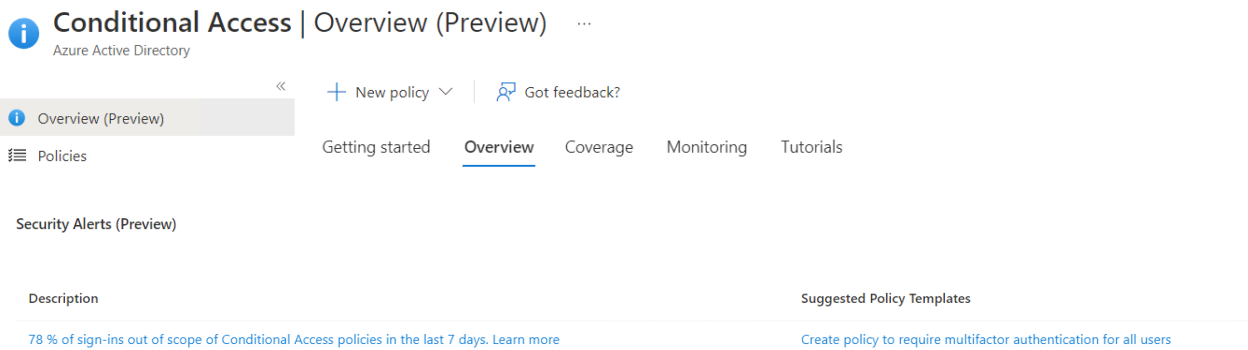
Conditional Access Management

All Conditional Policies will be enabled as **Report Only**, in other words, Policy will only record which User-Devices does not meet Requirements of the Policy. Change policy enforcement to **Yes** it's a must after deployment, but check user's configuration before apply to avoid lockouts.

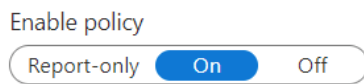
To access Conditional Access Policies type on the search box "Conditional Access" and select "Azure AD Conditional Access".



- **Edit Policy:** On Conditional Access Section you will see a list of Policies deployed on your tenant (Enabled or Disabled). To Edit a Policy Simple click on the desired Policy.
- **Check Policy Status:** On Overview tab you can check current status of every CA rule, in Security Alerts you can easy check a quick resume of compliance/noncompliance users-devices.



- **Enforce Policy:** On CA Policy Editor you can change From Report-Only to Enable or Disable options.



Runbooks

Runbooks can be found under Automation Account, Runbooks Section on left bar.

core | Runbooks ✕ ...

[+](#) Create a runbook
 [📄](#) Import a runbook
 [📖](#) Browse gallery
 [📄](#) Learn more
 [🔄](#) Refresh

🔍 Search runbooks...

Runbook type : All Authoring Status : All Runtime version : 7 selected

Showing 1 to 2 of 2 records.

| Name | Authoring status | Runbook type | Runtime version | Last modified | Tags |
|------------------|------------------|--------------|-----------------|-----------------|------|
| EXO-SS-CONFIGv21 | Published | PowerShell | 7.1 (preview) | 1/9/2022, 18:18 | |
| EXO-SS-DLPSv21 | Published | PowerShell | 7.1 (preview) | 1/9/2022, 18:18 | |

- Manage a Runbook: Click on any runbook and a new section will be open with all the options available to run, edit, delete or check runbooks status.

EXO-SS-CONFIGv21 (AutomationSecureScore/EXO-SS-CONFIGv21) ✕ ...

Runbook

🔍 Search (Ctrl+F) ⏪ Start 🔍 View ✎ Edit ⌚ Link to schedule ➕ Add webhook 🗑️ Delete 📄 Export 🔄 Refresh

Overview Essentials JSON View

Activity log Resource group : atsecurescore21ACC Subscription ID : 801151

Tags Account : AutomationSecureScore Status : Published

Diagnose and solve problems Location : Central US Runbook type : PowerShell

Resources Subscription : Microsoft Azure Runtime version : 7.1 (preview)

Jobs Tags (edit) : [Click here to add tags](#) Last modified : 1/9/2022, 18:18

Schedules Recent Jobs

Webhooks Status Created Last updated

Runbook settings No jobs found.

Properties

- Runbook Schedule: Click on any runbook and a new section will be open with all the options available to run, edit, delete or check runbooks status.
 - On left bar select “Resources”, “Schedule”
 - Click on “Add Schedule”

EXO-SS-CONFIGv21 (AutomationSecureScore/EXO-SS-CONFIGv21) | Schedules

Runbook

🔍 Search ⏪ + Add a schedule 🔄 Refresh

Overview Name Next run Time zone

Activity log No schedules found.

- Click on “Link a Schedule to your runbook”
- Select “Sec Daily Run”

Schedules ...

AutomationSecureScore/EXO-SS-CONFIGv21

+ Add a schedule

| Name | Next run | Time zone |
|---------------|------------------|----------------------------|
| Sec Daily Run | 22/9/2022, 23:59 | Coordinated Universal Time |

Runbook Monitoring

Advanced options will allow us to connect Automation Account with a desired Analytics Workspace. To trigger event on the analytics workspace some manual steps must be done..

- Enabling Monitoring:

- Go to **“Automation Account”** section on **“Secure Score”** Resource Group.
- On left bar select **“Monitoring”** and **“Diagnostic Settings”**
- Click on **“Add Diagnostic Settings”**

Diagnostic settings

| Name | Storage account | Event hub | Log Analytics workspa... | Partner solution | Edit setting |
|--|-----------------|-----------|--------------------------|------------------|--------------|
| No diagnostic settings defined | | | | | |
| + Add diagnostic setting | | | | | |

- Select Category to be audited, Diagnostic Name and Send to desired Analytics Workspace. Save and Close

Diagnostic setting name *

Logs

Category groups ⓘ

allLogs audit

Categories

JobLogs

JobStreams

DscNodeStatus

AuditEvent

Metrics

AllMetrics

Destination details

Send to Log Analytics workspace

Subscription

Log Analytics workspace

Archive to a storage account

Stream to an event hub

Send to partner solution

- On left bar select **“Monitoring”** and **“Alerts”**
- Click on **“Create Alert Rule”**
- Select **“Custom Role Search”**

Create an alert rule ...

Scope Condition Actions Details Tags Re

Configure when the alert rule should trigger by selecting a sig

+ Add condition

Choose a signal below and configure the logic on the next screen to define the alert condition.

Signal type 

All 

Monitor service 

All 

Displaying 1 - 11 signals out of total 11 signals

 Search by signal name

| Signal name |  Signal type |  Monitor service  |
|-----------------------------------|---|---|
| Custom log search |  Log search | Log analytics |

Create an alert rule ...

Scope Condition Actions Details Tags Review + create

Configure when the alert rule should trigger by selecting a signal and defining its logic.


Define the logic for triggering an alert. Use the chart to view trends in the data. [Learn more](#)

Log query

The query to run on this resource's logs. The results returned by this query are used to populate the alert definition below.

Search query *

 The value must not be empty.

[View result and edit query in Logs](#) 

Measurement

Select how to summarize the results. We try to detect summarized data from the query results automatically.

Measure 

Table rows 

[Review + create](#)

[Previous](#)

[Next: Actions >](#)

- Add this query to search for Failed tasks:

AzureDiagnostics | where ResourceProvider == "MICROSOFT.AUTOMATION" and Category == "JobLogs" and (ResultType == "Failed" or ResultType == "Stopped" or ResultType == "Suspended") | project TimeGenerated , RunbookName_s , ResultType , Resource

- Click on **“Review and Create”**

Troubleshooting

In some scenarios, automated connection or log output could present and undesired format or exit. Here is a list of potential problems if your environment does not have common configurations.

1. Runbook error while connecting (Service Principal resource is disabled):

```
| tokens from being issued for it. Trace ID:  
at Microsoft.Exchange.Management.AdminApiProvider.Authentication.MSALTokenProvider.GetAccessTokenAsync(String claims, String cmdletId)  
StatusCode: 400  
| a4926db-5670-48ef-b544-59c2a7818402 Correlation ID:  
ResponseBody: {"error": "invalid_resource", "error_description": "AADSTS50014: The service principal for resource 'https://ps.compliance.protection.outlook.com' is disabled.  
s indicate that a subscription within the tenant has lapsed, or that the administrator for this tenant has disabled the application, preventing tokens from being issued for
```

Cause: Exchange Application is disabled. Follow this steps to enable it.

Method 1: [Enable Exchange Online with Powershell](#)

Method 2: [Enable Exchange Online manually](#)

2. Runbook error while connecting (Tenant/User doesn't have valid plans):

```
ResourceUnavailable: C:\ModulesV2\User\ExchangeOnlineManagement\netCore\ExchangeOnlineM  
Line |  
754 |         throw $_.Exception;  
      |         ~~~~~  
      | Processing data from remote server  
      | nam10b.ps.compliance.protection.outlook.com failed with the following  
      | error message: Tenant/User doesn't have valid plans to use this Service.  
      | For more information, see the about_Remote_Troubleshooting Help topic.
```

Cause: There is no 365 environment/license configured.