



---

# Next-Gen Solutions Factory

Modern Workplace with Secure Score V2.1 Quick Start Guide

# SMB Fraud Defense UI View

**Location**

Select data center location

Select an available Azure Region

Resource Group name

First section of our Click-to-Run™ solution, a Resource Group Location and Name must be selected. This Resource Group will contain all required features of the Solution.

Select Domain ⓘ

Domain

Please select a domain

Current Security Defaults Status ⓘ

DISABLED

A list of available Domains in your environment will be shown. To configure 365 parameters a Domain must be selected.

This Section shows current status of Security Defaults, our recommendation is turn it on. However, if Security Defaults is disabled and Azure AD License is P1 or P2, Conditional Access Policies are available.

**Conditional Access Policies:** To be able to enable conditional access polices security defaults needs to be disabled and active AAD premium license.



Deployment Type | Azure AD | 365 Security | Advanced Options

Select Deployment ⓘ

Secure Score without Security Defaults ←

Secure Score without Security Defaults

Modern Secure Score with Security Defaults ←

**Please note:** This option is for scenarios where Security Defaults are enabled. Automation will only be for 365 parameters. Please refer to the step-by-step guide for details on how to enable.

No, I do not accept the above license consent

**Secure Score without Security Defaults:** This option allows to deploy Conditional Access Policies.

**Modern Secure Score with Security Defaults:** This option does not allow to deploy Conditional Access Policies.

Deployment Type | Azure AD | User Security | 365 Security | Advanced Options

Conditional Access Policies: Requires MFA for All Users ⓘ ←

Conditional Access Policy: Requires MFA [Exception: BreakGlass Group] ⓘ ←

**Conditional Access Policies: Requires MFA for All Users.**

**Conditional Access Policies: Requires MFA [Exception: BreakGlass Group] :** If BreakGlass Group is created or already exists on the tenant, that policy will create an exception for that Group.

# Azure AD Configuration: A new Service Principal must be created.

Deployment Type | **Azure AD** | User Security | 365 Security | Advanced Options

**Automation Account** ⓘ

AutomationSecureScore

**Create Break Glass Group?** ⓘ ←

**Create Certificate Password** ⓘ ←

Certificate Password

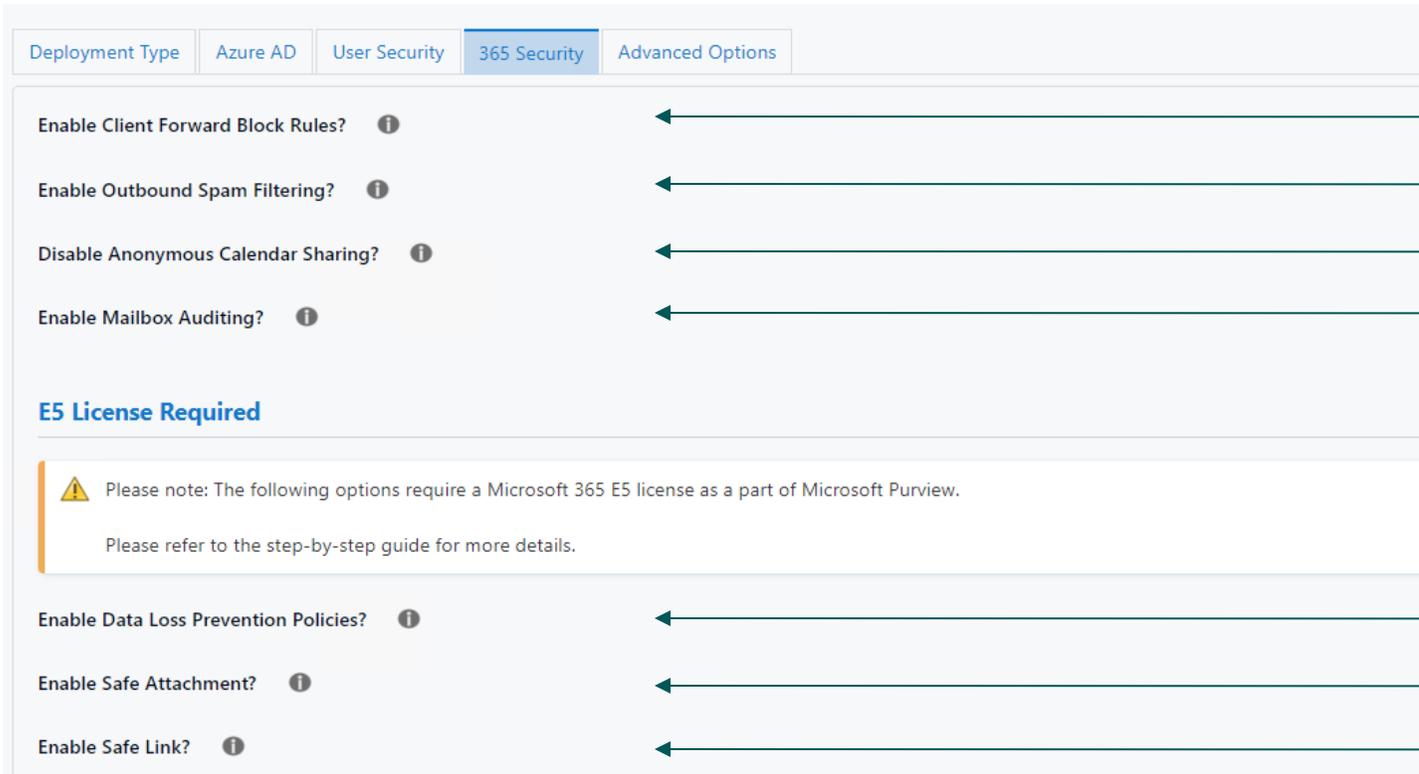
Confirm Password

Enter again your password

**Create BreakGlass Group:** This option allows to create a new Group for add exceptions on Conditional Access Policies.

**Create Password:** This password will be used to create a Self-Signed Certificate to validate AutomationSecureScore account with Azure AD.

## 365 Configuration: Allow to enable-disable different items to manage on Office 365. Some of the configurations will require a E5 license.



The screenshot shows the Microsoft 365 Security configuration interface. At the top, there are tabs for 'Deployment Type', 'Azure AD', 'User Security', '365 Security' (which is selected), and 'Advanced Options'. Below the tabs, there are four configuration options, each with an information icon (i) to its right:

- Enable Client Forward Block Rules?
- Enable Outbound Spam Filtering?
- Disable Anonymous Calendar Sharing?
- Enable Mailbox Auditing?

Below these options is a section titled 'E5 License Required' with a warning icon (⚠) and 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.'

At the bottom, there are three more configuration options, each with an information icon (i) to its right:

- Enable Data Loss Prevention Policies?
- Enable Safe Attachment?
- Enable Safe Link?

Red arrows point from the explanatory text on the right to the information icons of the corresponding configuration options.

**Client Forward Block:** This option allows to protect against uncontrolled forwards.

**Outbound Spam Filtering:** This option allows to protect against forward spamming.

**Anonymous Mailbox Sharing:** This option allows to disable anonymous calendar access.

**Mailbox Auditing:** This option allows to audit mailboxes.

**Data Loss Prevention:** This option allows to Deploy specific DLPS by country or region.

**Safe Attachments:** This option allows to protect against attachments.

**Safe Links:** This option allows to protect against links on emails.

## Advanced Options



Deployment Type | Azure AD | User Security | 365 Security | **Advanced Options**

Enable Runbook Monitoring? ⓘ

Enable Daily Automation Scheduling? ⓘ

 Please note: If you select No, the automation will not run until you schedule manually.  
Please refer to step by step guide for details on how to enable it.

Enable Advanced Options? ⓘ

No, I do not accept the above license consent

**Runbooks Monitoring:** This option allows to connect Automation Account with existing Log Analytics Workspaces (manual steps required).

**Daily Automation Scheduling:** This option allow to schedule Automation Account execution every 6 hours, (manual step required to select which runbooks must be executed).

**Advance Options (BYOC):** This option allows to upload custom code as a runbook.