CISA's SCuBA & BINDING OPERATIONAL DIRECTIVE 25-01

MARCH 31, 2025

Roger Mamika
March 31, 2025

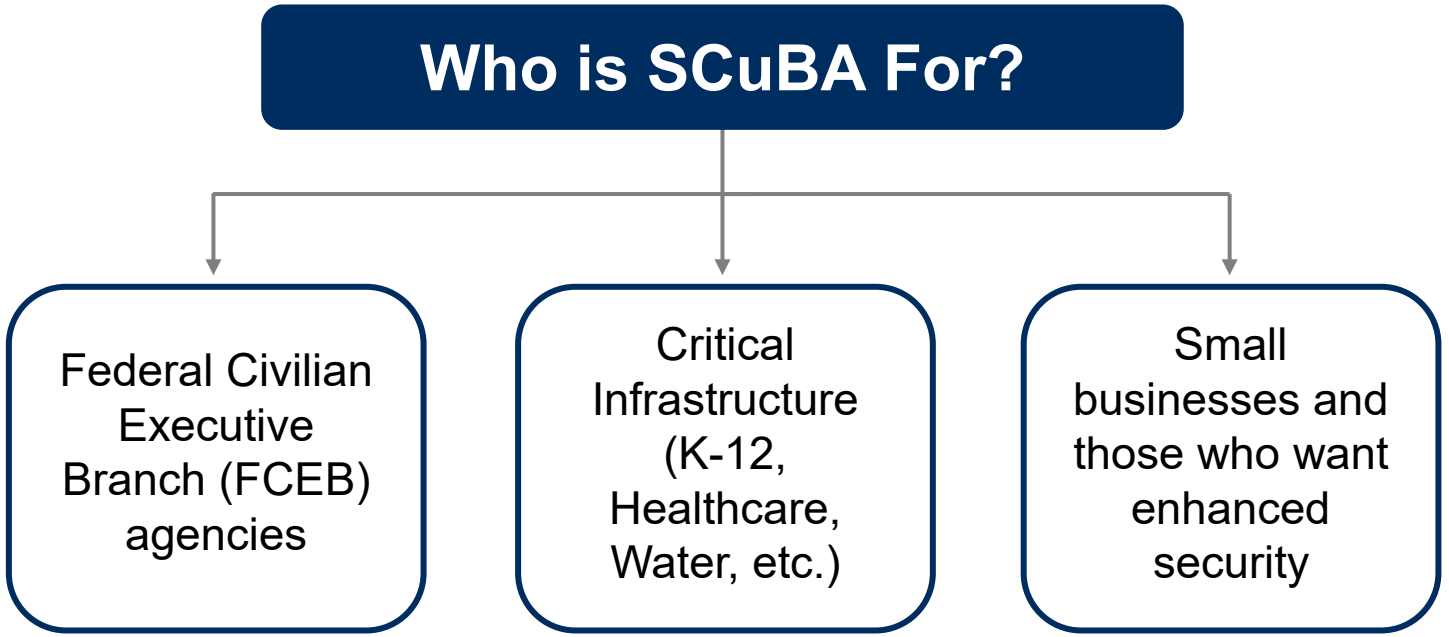
TLP: CLEAR

SCuBA Overview

- SCuBA enhances the security of cloud business application environments through added configurations, settings, and security products.
- This **comprehensive approach** ensures robust and reliable resources that can rapidly adapt to the constant changes, updates and threats common in Software as a Service (SaaS) offerings.
- Open source and offered at no cost to FCEB agencies, Critical Infrastructure (CI) organizations, and private organizations.

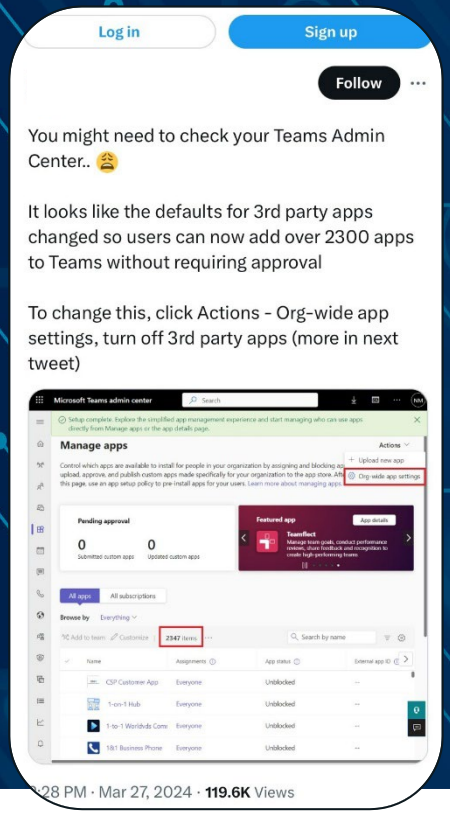
WHAT IS SCuBA?

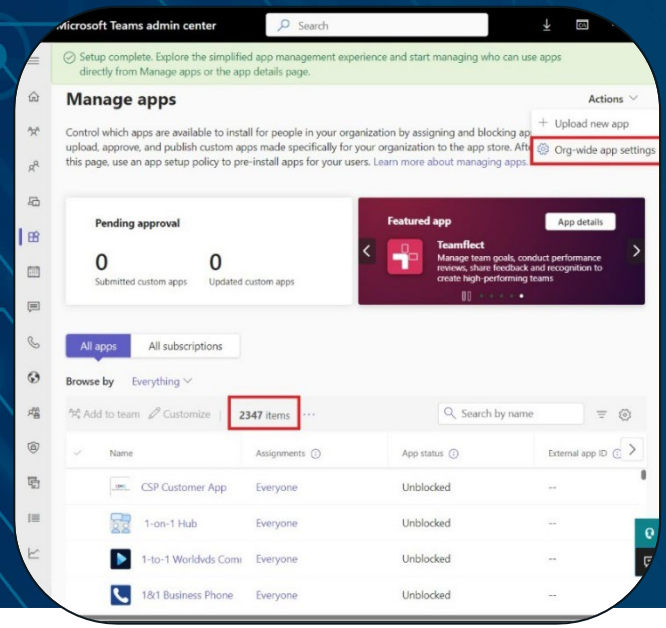
The Secure Cloud Business Applications (SCuBA) project provides guidance and capabilities to secure your organization's cloud business application environments. The service was developed with a comprehensive threat-informed methodology to identify cloud visibility coverage gaps and requirements.



TLP: CLEAR

WHY SCuBA?





Many default configurations could result in security compromises. Organizations using ScubaGear can assess their configurations against SCuBA-developed security baselines to improve their cloud security compliance.

Roger Mamika
March 31, 2025

TLP: CLEAR

ScubaGear & ScubaGoggles Overview

- On December 12, 2023, CISA SCuBA published its first draft Google Workspace (GWS) Secure Configuration Baselines (SCBs) and the GWS assessment tool called **ScubaGoggles** for public comment on CISA.gov/scuba and https://github.com/cisagov/scubagoggles.
- The Microsoft 365 (M365) SCBs were published on December 21, 2023. Pilot engagements and RFC comments informed key improvements made to the security configuration guidance and **ScubaGear** tool.
- Both tools:
  - **Compare tenant configurations** to CISA's security recommendations.*
  - **Lower the amount of effort** required for entities to assess themselves, providing a detailed report.
  - Have code updates that will be **released on a regular basis** to address Google's and Microsoft's configuration updates.
  - Allow for CISA **real-time visibility into tenant configuration** (Multi-Tenant Application).
  - Do not collect data or share data with CISA; they only create output reports.

By the Numbers

As of 2/27/25

M365

- 7 Secure Configuration Baselines
- Over 1,900 GitHub Stars
- 75,716 downloads of v1.4.0
- 126,405 total downloads across all releases

GWS

- 9 Secure Configuration Baselines
- 197 GitHub Stars
- 52 downloads of v0.4.1
- 1,005 downloads across all releases

GWS SCB guidance does not cover Google services outside of GWS (e.g., Maps, Photos) or any GWS Marketplace Apps created by third-party developers.

TLP: CLEAR

Product-Specific Security Baselines

Microsoft 365

- ✓ Entra ID/Azure Active Directory
- ✓ Defender for Office 365
- ✓ Exchange Online
- ✓ Power BI
- ✓ Power Platform
- ✓ SharePoint Online + OneDrive for Business
- ✓ Teams

Google Workspace

- ✓ Gmail
- ✓ Common Controls
- ✓ Drive/Docs
- ✓ Meet
- ✓ Chat and Classic Hangouts
- ✓ Calendar
- ✓ Groups for Business
- ✓ Sites
- ✓ Classroom

M365 Baselines and ScubaGear

Baselines

Baselines	Permissions
Entra ID/Azure Active Directory	Global Reader
Exchange Online	Global Reader (Or Exchange Administrator)
Defender for Office 365	Global Reader (Or Exchange Administrator)
OneDrive for Business	N/A
SharePoint Online	SharePoint Administrator
Microsoft Teams	Global Reader (or Teams Administrator)
Power BI	N/A
Power Platform	Power Platform Administrator with a “Power Apps for Office 365” License

- **License Assumption:** M365 G3; some controls require add-ons
- **Severity Levels:** SHALL and SHOULD language dictates severity level

ScubaGear

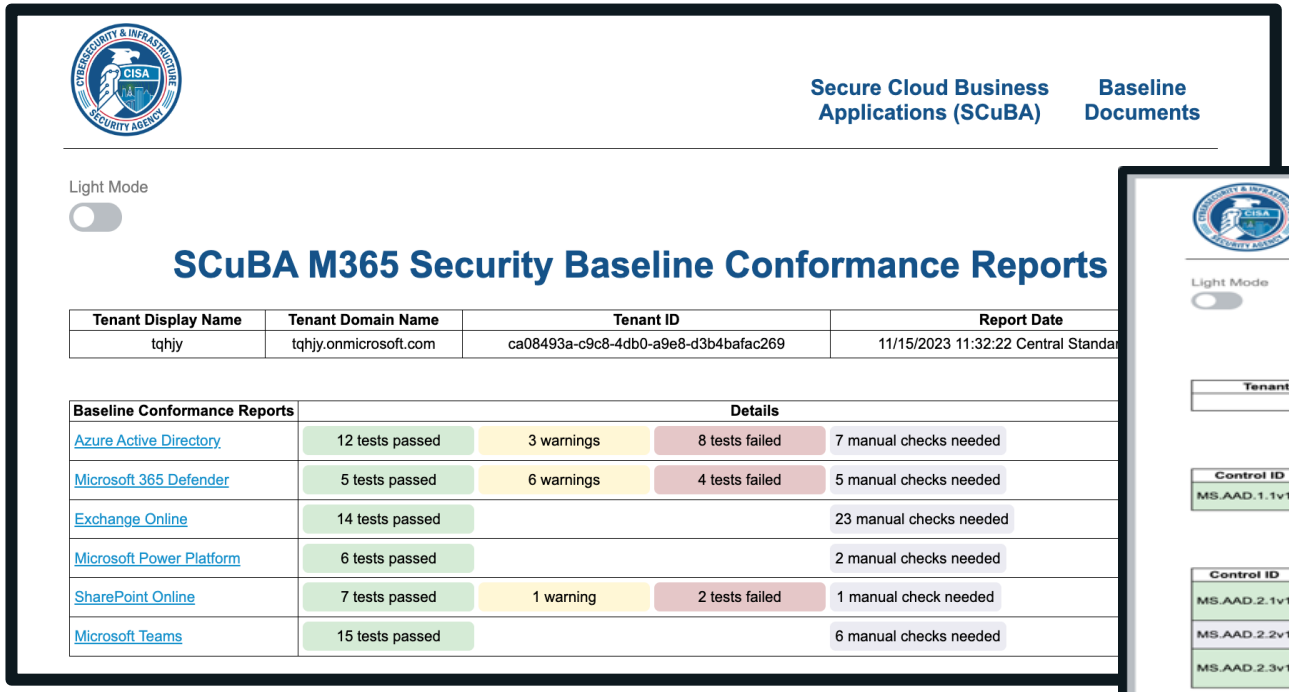
- Compares agency tenant configurations to CISA’s security recommendations.
- Lowers the amount of effort required for entities to assess their tenant configuration, providing a detailed report.
- Code updates will be released on a regular basis to address Microsoft configuration drift.
- Four major releases and one minor release since Dec. 22, 2023.

https://github.com/cisagov/ScubaGear

SCBs Outline Each Policy with Supporting Criteria

Policy	Criteria	Description of Criteria
	Category	A common category to which the SCB policy applies (e.g., Secure Passwords)
	Policy Description	Uses the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL“. Key words are to be interpreted as described in IETF RFC 2119.
	Rationale	Rationale describing why the policy should be implemented
	MITRE ATT&CK TTP Mapping*	Lists related Adversary Behaviors from MITRE ATT&CK (Tactics, Techniques, and Procedures) where the described SCB policy provides defense coverage
	Resources	Links to resources supporting policy or implementation
	Prerequisites	Describes any prerequisites that need to be configured prior to implementation
	Implementation	Steps on how to execute the policy in M365

ScubaGear | Sample Summary Reports



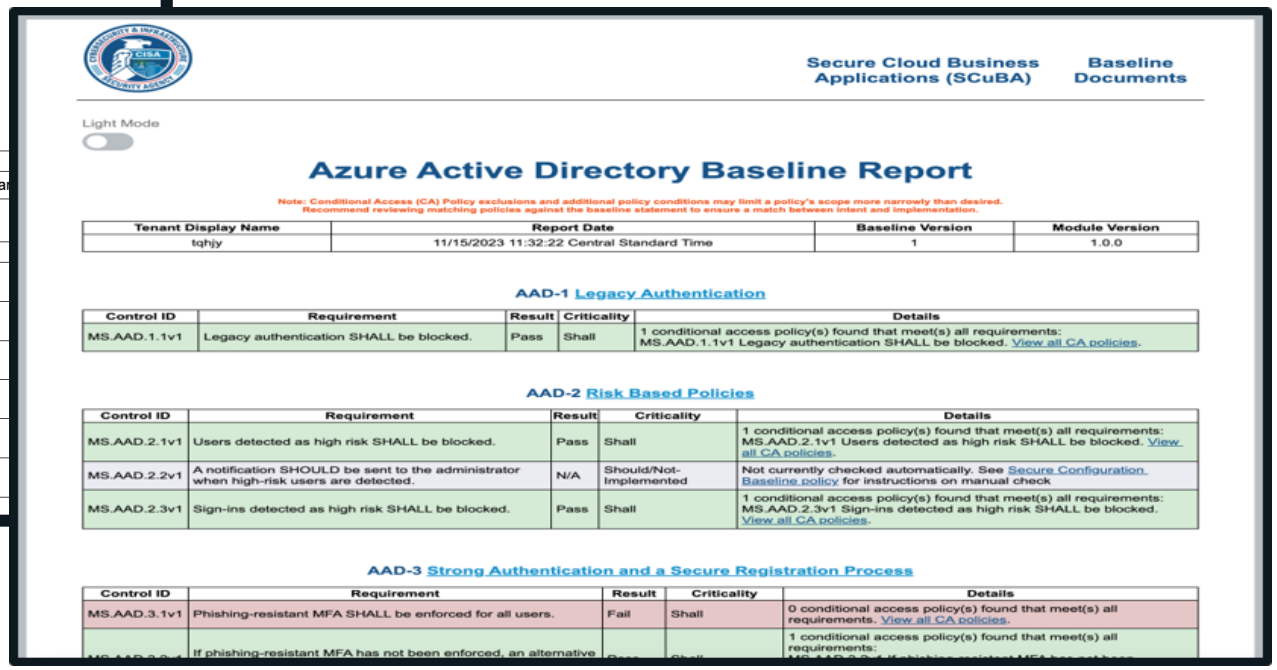
Secure Cloud Business Applications (SCuBA) | Baseline Documents

Light Mode

SCuBA M365 Security Baseline Conformance Reports

Tenant Display Name	Tenant Domain Name	Tenant ID	Report Date
tqhjy	tqhjy.onmicrosoft.com	ca08493a-c9c8-4db0-a9e8-d3b4bafac269	11/15/2023 11:32:22 Central Standar

Baseline Conformance Reports	Details			
Azure Active Directory	12 tests passed	3 warnings	8 tests failed	7 manual checks needed
Microsoft 365 Defender	5 tests passed	6 warnings	4 tests failed	5 manual checks needed
Exchange Online	14 tests passed			23 manual checks needed
Microsoft Power Platform	6 tests passed			2 manual checks needed
SharePoint Online	7 tests passed	1 warning	2 tests failed	1 manual check needed
Microsoft Teams	15 tests passed			6 manual checks needed



Secure Cloud Business Applications (SCuBA) | Baseline Documents

Light Mode

Azure Active Directory Baseline Report

Note: Conditional Access (CA) Policy exclusions and additional policy conditions may limit a policy's scope more narrowly than desired. Recommend reviewing matching policies against the baseline statement to ensure a match between intent and implementation.

Tenant Display Name	Report Date	Baseline Version	Module Version
tqhjy	11/15/2023 11:32:22 Central Standard Time	1	1.0.0

AAD-1 Legacy Authentication

Control ID	Requirement	Result	Criticality	Details
MS.AAD.1.1v1	Legacy authentication SHALL be blocked.	Pass	Shall	1 conditional access policy(s) found that meet(s) all requirements: MS.AAD.1.1v1 Legacy authentication SHALL be blocked. View all CA policies.

AAD-2 Risk Based Policies

Control ID	Requirement	Result	Criticality	Details
MS.AAD.2.1v1	Users detected as high risk SHALL be blocked.	Pass	Shall	1 conditional access policy(s) found that meet(s) all requirements: MS.AAD.2.1v1 Users detected as high risk SHALL be blocked. View all CA policies.
MS.AAD.2.2v1	A notification SHOULD be sent to the administrator when high-risk users are detected.	N/A	Should/Not-Implemented	Not currently checked automatically. See Secure Configuration Baseline policy for instructions on manual check
MS.AAD.2.3v1	Sign-ins detected as high risk SHALL be blocked.	Pass	Shall	1 conditional access policy(s) found that meet(s) all requirements: MS.AAD.2.3v1 Sign-ins detected as high risk SHALL be blocked. View all CA policies.

AAD-3 Strong Authentication and a Secure Registration Process

Control ID	Requirement	Result	Criticality	Details
MS.AAD.3.1v1	Phishing-resistant MFA SHALL be enforced for all users.	Fail	Shall	0 conditional access policy(s) found that meet(s) all requirements. View all CA policies.
	If phishing-resistant MFA has not been enforced, an alternative			1 conditional access policy(s) found that meet(s) all requirements:

The summary reports provide an accessible and user-friendly interface.
No information or data is automatically sent to CISA.
Power Platform and SharePoint admin roles are required to generate individual service reports.

BOD 25-01 Live Walkthrough of Supporting Pages and Content

Roger Mamika
March 31, 2025

TLP: CLEAR

SCuBA Contact and Resources

For questions, email scuba@cisa.dhs.gov

github.com/cisagov/ScubaGear

github.com/cisagov/ScubaGoggles