

ALEA OVERSEAS N.V. Information Security Policy

Creation date: 19/05/2020

Version: 2.5

From: Compliance

To: ALEA Employees

Objective :

The purpose of this procedure is to safeguard the integrity, confidentiality, and availability of the information handled by ALEA OVERSEAS N.V.

Information Security Policy

Version 2.5

Version	Date	Author	Changes
1.0.	08-05-2020	Helene Klein – Compliance Officer	First version
1.1.	19-05-2020	Eduard Fumàs Cases – Chief Technology Officer	Including: • Back-end automatic log-off after a period of inactivity. • Safeguarding of applications
2.	15-09-2023	Eduard Fumàs Cases – Chief Technology Officer	Including: • Change Password Policy. • Added JAMF (Mobile Device Management). • Added OKTA (Identity Management).
2.1	28 Sep 2023	Jonathan Cho – Head of Legal	Amended company information
2.2	02-11-2023	Eduard Fumàs Cases – Chief Technology Officer	Including: - Changes on Internal Audit.
2.3	27 Nov 2023	Jonathan Cho – Head of Legal	Amended wording to include group company employees
2.4	11 Nov 2024	Eduard Fumàs Cases – Chief Technology Officer	Change password policy
2.5	20 May 2025	Eduard Fumàs Cases – Chief Technology Officer	Update Incident Response Team

Table of Contents

I. Purpose	6
I.1. Definition	6
I.2. Foreword	6
I.3. Objectives	6
I.4. Definition	7
II. Our Responsibilities	7
III. Acceptable Use Policy	9
IV. Disciplinary Action	10
V. Data Classification	10
VI. Data Protection	10
VII. Access to Sensitive Data	11
VIII. Login & Logoff Process	11
IX. Password Policy	12
X. Computer viruses, Worms, and Trojan horses	13
XI. Encryption	14
XII. Portable Device & Media	14
XIII. USB Storage Device	15
XIV. Email Usage	15
XIV.1. Sharing and forwarding	15
XIV.2. User identity	15
XIV.3. Content of message	15
XIV.4. Incidental disclosure	16
XIV.5. Public representations	16
XV. BYOD Policy – Bring Your Own Device	16
XVI. Physical Security	17
XVII. Disposal of Media & Equipment	18

XVIII. Security Awareness & Procedures	18
XIX. Teleworking Procedures	18
XX. Security Review Plan	19
XX.1. Independent Security Audit	19
XX.2. Permissions and access rights review	19
XX.3. Updates on gaming services	19
XXI. Social Media	20
XXII. Network & Remote Access	20
XXIII. Vulnerability Management Policy	20
XXIV. Incident Response Plan	21
XXV. Network Security	22
XXVI. Safeguarding of Equipment	22
XXVII. Clear Desk Policy	23
XXVIII. Communication of Policies	23
XXIX. Right of Erasure & Right to Access	23
XXX. Internal Audit	23
XXX.1. Introduction & Responsibility	23
XXX.2. Operational Internal Audit	24
XXXI. JAMF (Mobile Device Management)	24
XXXI.1.1. Advantages of MDM	25
XXXI.1.2. Why JAMF?	26
XXXII. OKTA (Identity Management)	27
XXXII.1.2. Why OKTA?	27
XXXII.1.2. OKTA Features	29
XXXII.1.3. Benefits of using OKTA?	30
XXXIII. Safeguarding of Applications	31
XXXIII.1. CMS	31
XXXIII.1.1. Introduction	31

XXXIII.1.2. How it Works?	32
XXXIII.1.3. Implementation	33
XXXIII.2. Launch-API & Customer-API	35
XXXI.2.1. What is JSON Web Token?	35
XXXI.2.2. Why are we using JSON Web Token?	35
XXXI.2.3. Custom Signature Header	35
XXXIII.3. Transaction-API & Transaction-API-Proxy	36
XXXI.3.1. Introduction	36
XXXI.3.2. How it works?	37
XXXIV. Back-end automatic log-off	38
XXXIV.1. Introduction	38
XXXIV.2. Token lifetime policy properties	39

I. Purpose

I.1. Definition

For the purpose of this Policy, “**ALEA Play**” refers to **ALEA OVERSEAS N.V.** (hereinafter “**ALEA**”) and its affiliated entities within the **ALEA Group of Companies**.

This Policy is specifically established for **ALEA OVERSEAS N.V.**, which operates under the trade name **ALEA Play**, and extends to all related group companies that are part of ALEA’s business operations.

I.2. Foreword

This document sets forth the information security framework for **ALEA OVERSEAS N.V.**, covering all aspects of the protection of information — whether confidential or not — belonging to ALEA and its group of companies.

It establishes management direction, procedural requirements, and technical guidelines to ensure the proper safeguarding of the ALEA Play information systems.

This Policy shall be reviewed annually, or as required, by ALEA Play Senior Management to ensure continuous compliance and effectiveness.

The Policy is distributed to all **ALEA employees** (including third-party contractors), who are required to read it in full and acknowledge their understanding by signing the corresponding form — either during onboarding or upon each policy update.

I.3. Objectives

By this Policy, we must make sure that:

- The Information Security Policy provides clear direction for the information security program.
- The Information Security Policy shows that management is committed to information security.
- Management supports the organization’s information security policy.
- The Information Security Policy shows that management is prepared to support an on-going commitment to information security.
- The Information Security Policy is consistent with the business objectives.

- The Information Security Policy meets the organization's business requirements.
- The Information Security Policy complies with all relevant laws and regulations and GDPR related requirement.

I.4. Definition

For clarification purpose, some terms used in this document are defined below:

- **"ALEA Play"** or **"the Company"** refers to **ALEA OVERSEAS N.V.** and all its subsidiaries within the ALEA Group. This definition also includes any third-party companies engaged under a direct service agreement with any ALEA Group entity that handle sensitive or personal data on ALEA's behalf.

For the avoidance of doubt, **"ALEA Play"** is the commercial and operational name used by **ALEA OVERSEAS N.V.**, and does not represent a separate legal entity.

- **"Employees"** should be understood as all employee of ALEA, including 3rd Party individuals engaged with ALEA through a service agreement.
- **"Sensitive data"** shall refer to any type of data, in whatever form, owned by ALEA Play, or shared by any 3rd Party for ALEA Play's activities and that are not public or common knowledge. Thus including, but not limited to, personal data as defined by the GDPR, but also ALEA Play's financial, contractual, and legal data.

II. Our Responsibilities

The CTO (Chief Technology Officer), or the maximum responsible of the Engineering Department, has been entrusted with direct responsibility for maintaining this Policy and providing advice on information security and guidance on its implementation.

All employees have a responsibility to conduct themselves in an ethical manner. In particular:

- Data/information obtained inappropriately should not be used.
- Finding a system weakness should be reported immediately and should not be taken advantage of.
- Every employee has a responsibility to carry out his/her work diligently and will be held accountable for misuse of the company's information system.
- When the confidentiality of information is unclear, its classification should be ascertained.

- Report any known violation or system weakness to person or persons responsible for security Information Security Policy.

ALEA Play handles personal and sensitive data daily. Information must have adequate safeguards in place to protect them, to protect our clients' and employees' privacy, to ensure compliance with various regulations and to guard the future of the organization.

Employees handling sensitive data should ensure:

- Handle Company and customer information in a manner that fits with their sensitivity.
- Limit personal use of the company information and telecommunication systems and ensure it does not interfere with your job performance.
- The Company reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems, and network traffic for any purpose.
- Do not use e-mail, internet, and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing, or illegal.
- Do not disclose personal information unless authorized in writing.
- Protect sensitive information.
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.
- Do not install unauthorized software or hardware, including modems and wireless access unless you have explicit management approval.
- Always leave desks clear of sensitive data and lock computer screens when unattended.
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.
- Do not disclosed any sensitive information, whether handled by ALEA or entrusted by a 3rd Party.
- Do not engaged, or otherwise use ALEA Information System, in hacking activities that include, but are not limited to, gaining unauthorized access to any information system (Managed by ALEA or not), altering, damaging, or otherwise obtaining password, encryption or other mechanism that could grant unauthorized access.
- Do not test or attempt to compromise any information system unless specifically authorized to do so by the CTO. Employees must not possess software or other tools that are designed to compromise information security.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorized access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

III. Acceptable Use Policy

The Management's intentions for publishing an acceptable use policy are not to impose restrictions that are contrary to the ALEA's established culture of openness, trust, and integrity.

Management is committed to protecting the employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

ALEA will maintain an approved list of technologies and devices and personnel with access to such devices:

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Employees should ensure that technologies should be used and setup in acceptable network locations.
- Keep passwords secure and do not share accounts. Only use the password management system ("Keeper") provided by ALEA.
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops, workstations, mobile and tablet should be secured with a password-protected screensaver with the automatic activation feature.
- All password/PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Because information contained on portable computers is especially vulnerable, particular care should be exercised.
- Postings by employees from a ALEA email address or account to newsgroups, forum or any social media should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Company, unless posting is during business duties.

- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

IV. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee may result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for noncompliance.

V. Data Classification

Data and media containing data must always be labelled to indicate sensitivity level:

- **Public:** Information is not confidential and can be made public without any implications from ALEA.
- **Shared:** Information is confidential but can be shared between ALEA and a 3rd party recipient. The information can be shared across ALEA and 3rd party peers but shall not be disclosed publicly.
- **Internal Use:** Information is restricted to ALEA and can freely be shared across ALEA employees. Those data should however be protected from external access and shall not be disclosed externally without prior written consent of ALEA.
- **Confidential:** These are information which there are legal or strategic requirements for preventing disclosure or financial penalties for disclosure. Confidential data includes data collected by ALEA and tied to a privacy statement.

In addition to the above, the following classification should be applied by default:

- Business peer-to-peer communication such as, but not limited to, email and Chat should be considered “Shared” unless otherwise specified.
- Any document produced by ALEA should be considered “Internal Use” unless otherwise specified.

Any document containing Personally Identifiable Information (In the sense of the GDPR), whether it is ALEA customer’s or employee’s data, should be considered “Confidential”.

VI. Data Protection

All sensitive data stored and handled by ALEA and its employees must be securely always protected against unauthorized use.

Any sensitive data that is no longer required by the Company for business reasons must be discarded in a secure and irrecoverable manner:

- If there is no specific need to see personal or sensitive data, it must be masked when displayed.
- ALEA employees must not disclose sensitive data outside the ALEA premises and messaging systems (Chat, Mail, Skype, etc.), unless duly authorized to do so in writings by the ALEA management.

It is strictly prohibited to:

- To print/store hard copies of any sensitive data, unless otherwise required for legal or regulatory reasons.
- To print/write credentials allowing to access ALEA systems.

Any confidential documents should be stored in a safe place, or in a cabinet which is locked and only accessible to authorized people.

Also, Data protection is the process of safeguarding important information from corruption, compromise, or loss. Data protection strategies are evolving along two lines: data availability and data management.

Data availability ensures users have the data they need to conduct business even if the data is damaged or lost. For this reason, in ALEA we have a procedure “Business Continuity & Disaster Recovery” + “Data Backup” to ensure the availability of the data.

When data is corrupted or accidentally deleted, we use the snapshots generated to restore the database. You can find all the information of this procedure on “Data Backup Procedure”.

VII. Access to Sensitive Data

All access to sensitive data should be controlled and authorized. Access to sensitive data is granted to individual according to their role, as defined in the document “Human Resources Roles & Responsibilities”. So, it means that all data is safeguarded against unauthorised access.

VIII. Login & Logoff Process

All users must be positively identified prior to being able to use any ALEA computer or communications system resources.

In case for rooms with single occupation, the room must be locked. In case a user forgets to lock their computer, if there has been no activity on a computer terminal, workstation, or personal computer for a certain period, the system must automatically blank the screen and suspend the session. Reestablishment of the session must take place only after the user has provided a valid password.

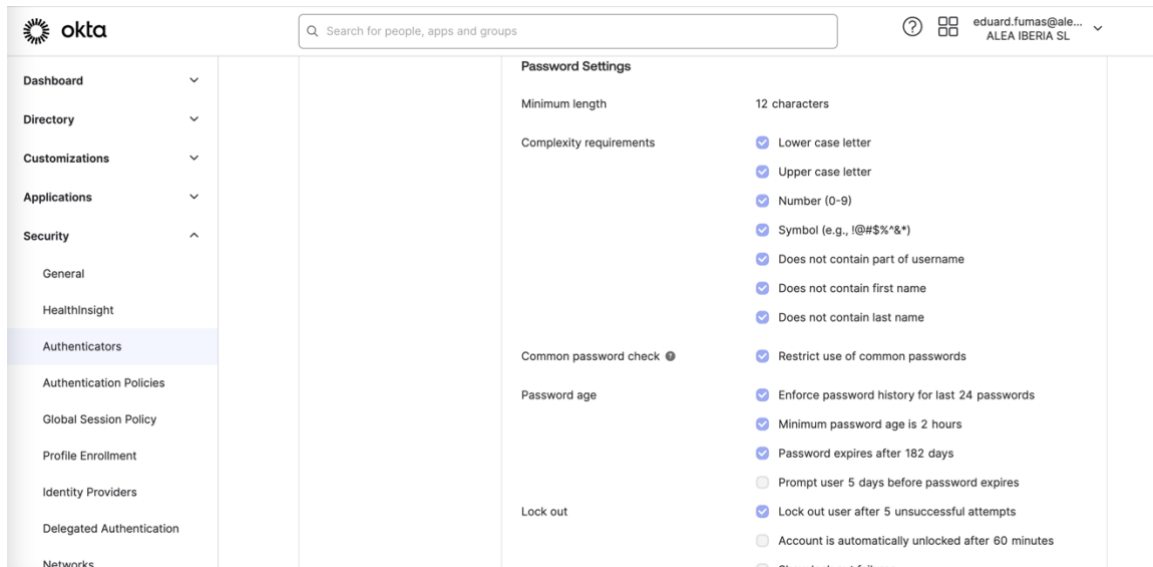
An exception to this policy will be made in those cases where the immediate area surrounding a system is physically secured by locked doors, secured-room badge readers, or similar technology. All other users must lock their computer whenever they leave their desk.

Using someone else credential to connect to any ALEA system is strictly prohibited. Using a workstation logged with such account shall not be permitted.

IX. Password Policy

With the exclusion of service accounts, the following policy should be applied for ALEA Play corporate (domain-based password):

- The password should contain a minimum of 12 characters.
- Password complexity requirement should be enabled whenever possible (usually at least one upper case letter, one number and one symbol).
- The password maximum age is 6 months, and a previous password cannot be reused.
- In the event of 5 consecutive failed login, the related account should be locked out for a minimum of an hour.



X. Computer viruses, Worms, and Trojan horses

Approved and current virus-screening software must be enabled on ALEA computer systems. This software must be used to scan all software coming from third parties or other departments and must take place before the new software is executed. Users must not bypass scanning processes that could stop the transmission of computer viruses.

The introduction of computer viruses or disruptive/destructive programs into the ALEA environment is prohibited, and violators may be subject to prosecution.

The Engineering Department is responsible for eradicating viruses from all personal computer systems. As soon as a virus is detected, the involved user must immediately notify the Engineering department to assure that no further infection takes place and that any experts needed to eradicate the virus are promptly engaged.

ALEA computers and networks must not run software that comes from sources other than business partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from un-trusted sources must not be used unless it has been subjected to a rigorous testing regimen approved by the Engineering Department.

Headers of all incoming data including electronic mail must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.

Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

XI. Encryption

When sensitive information is transmitted over any communication network, it must be sent in encrypted form. Whenever information is stored or transported in computer-readable storage media, it must also be in encrypted form.

Encryption of information in storage or in transit must be achieved through commercially available products approved by the Engineering Department.

Encryption keys used for ALEA information are always classified as Confidential information. Access to such keys must be limited only to those who have a need to know. Unless the approval of the CTO or the maximum responsible of Engineering Department, is obtained, encryption keys must not be revealed to consultants, contractors, temporaries, or other 3rd Parties.

Wireless networks in use must always be configured to employ encryption. Any form of sensitive or transactional data transmitted from/to the online system must be encrypted.

XII. Portable Device & Media

Users in the possession of portable, laptop, notebook, handheld, and other transportable computers and/or media containing sensitive information, must not leave these computers/media unattended at any time unless the information is stored in encrypted form. Users in the possession of transportable computers containing unencrypted confidential data must not check these computers in airline luggage systems or with hotel porters. These computers must remain in the possession of the traveller as hand luggage.

In addition to the present “Information Security Policy”, any employee in a possession of a portable device owned by ALEA Play should sign the device loaner agreement “Device Loaner Agreement”.

XIII. USB Storage Device

Due to the risk, they introduce, and notably virus threats and data leak, the usage of USB device is not authorized on ALEA. Also, the usage of USB storages including, but not limited to, USB keys and USB Hard drives, is not authorized.

XIV. Email Usage

XIV.1. Sharing and forwarding

Electronic mail accounts, like user IDs, are for specific individuals and must not be shared. If a user goes on vacation or is otherwise unable to check their mail for extended periods, mail can be forwarded to another ALEA employee with the exclusion of 3rd parties. Notices can be established that will automatically inform correspondents that the recipient will not be responding for a certain period. Upon departure from ALEA, employee electronic mail account must be terminated, and email erased.

If an electronic mail message contains sensitive information, users must not forward it to another recipient unless the other recipient is known to be authorized to view the information, or the originator approves the forwarding. Broadcast electronic mail message facilities must not be employed unless department manager approval is obtained, but the use of selected distribution lists (if these exist) is both advisable and permissible without such approval.

XIV.2. User identity

Misrepresenting, obscuring, suppressing, or replacing another user's identity on an electronic communications system is forbidden. The username, electronic mail address, organizational affiliation and related information included with electronic messages or postings must reflect the actual originator of the messages or postings.

Except for a generic email, such as customer support services that may be anonymous, users must not send anonymous electronic communications. At a minimum, all users must provide their name and phone number in all electronic communications. Electronic mail signatures indicating job title, company affiliation, address and other particulars are strongly recommended for all electronic mail messages. Digital certificates are also recommended for electronic mail.

XIV.3. Content of message

Users must not use profanity, obscenities, or derogatory remarks in any electronic mail messages discussing employees, customers, competitors, or others involved with ALEA business. Such remarks may create legal problems such as trade libel and defamation of character. Special caution is warranted because backup and archival copies of electronic mail made by third parties may be more permanent and more readily accessible than traditional paper communications.

XIV.4. Incidental disclosure

ALEA information systems must not be used for the exercise of a user's right to free speech. Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. Users must respond directly to the originator of offensive electronic mail messages, telephone calls, or other communications. If the originator does not promptly stop sending offensive messages, users must report the communications to their manager and to Human Resources.

XIV.5. Public representations

No media advertisement, Internet home page, electronic bulletin board posting, electronic mail message, voice mail message, or any other public representation about ALEA may be issued unless prior approval has been granted by the authorized department's manager.

ALEA, as a matter of policy, does not send unsolicited electronic mail, nor does it issue unsolicited fax advertising. Nobody outside ALEA may be placed on an electronic mail distribution list without indicating their intention to be included on the list through an opt-in process. If ALEA users are bothered by an excessive number of unwanted messages from a particular organization or electronic mail address, they must not respond directly to the sender.

Recipients must forward samples of the messages to the Engineering Helpdesk support for resolution. Users must not send large number of messages to overload a server or user's electronic mailbox in retaliation for any perceived issue.

XV. BYOD Policy – Bring Your Own Device

ALEA allows the use of personally owned devices (non-corporate devices) if the devices follow the same rules and practice than described in:

- Acceptable use policy
- Data classification

- Protect stored data.
- Logon and logoff process
- Computer viruses, worms, and Trojan horses
- Encryption
- Portable device and media
- Disposal of media & equipment

However, such usage is under the employee responsibility that should make sure to respect with the rules and practice. Failing to comply may result to the same disciplinary action as defined in this document “Information Security Policy”.

XVI. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data:

- Employees are responsible for exercising good judgement regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorized access to Confidential or Internal Only data.
- Employees should ensure that technologies should be used and setup in acceptable network locations.
- A list of ALEA devices should be maintained.
- The list should include make, model, and location of the device.
- The list should have the serial number or a unique identifier of the device.
- The list should be updated when devices are added, removed, or relocated.
- Personnel using the devices should verify the identity of any 3rd party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.
- Keep passwords/PIN secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Media containing sensitive data information must be handled and distributed in a secure manner by trusted individuals.

- Strict control is maintained over the external or internal distribution of any media containing sensitive data and must be approved by management.
- Strict control is maintained over the storage and accessibility of media.
- All computer that stores sensitive data must have a password protected screensaver enabled to prevent unauthorized use.

XVII. Disposal of Media & Equipment

Should any media that is no longer required due to numerous reasons, such as excess of useful life, change in requirements, damage, inability to upgrade, non-viable maintenance cost or simply replacement by new hardware must be checked by the Engineering Department to ensure that no sensitive information is held on the device.

If the item is non-salvageable i.e., no parts can be used for other maintenance purposes, the Engineering Department would need to dispose of the equipment. The members of the Engineering Department would need to ensure that data is erased from the equipment by securely overwriting the data, while the CTO, or the maximum responsible of the Engineering Department would need to authorize the release of the equipment.

Should hardware within the datacentre needs to be removed, the Asset Removal Policy outlines the steps carried out to remove such hardware.

XVIII. Security Awareness & Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain security awareness. The protection of sensitive data demands regular training (yearly based) of all employees, including service contractor that access to sensitive data:

- Company security policies must be reviewed annually and updated as needed.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form.

XIX. Teleworking Procedures

Each worker has the option to work from home 24 days per year. Those days must be agreed & approved by his/her the direct Manager.

Workers can take laptop and mobile to work remotely. While the devices are out of the office, they must respect security best practices:

- Do not leave the device unattended. Do not leave device in a car or in a hotel's room. In case of hotel, leave it in the safe if it is possible.
- Do not connect to any unsecure Wi-Fi. It is forbidden to connect to any Wi-Fi without security settings. The home's access point must have strong security settings.
- Do not allow other people use company's devices.
- Do not use company's devices for non-working purposes. (Surfing internet or installing non-work-related software)
- In case of device's failure, ask first to company's system administrator before going to any repair store.

Other portable devices policies are defined in the document "Device Loaner Agreement". More can be found about the Teleworking from the "Benefits Procedure".

XX. Security Review Plan

Security reviews will be organized and performed by the Engineering Team to make sure that the security policies and procedures are being fulfilled.

XX.1. Independent Security Audit

A third-party company will carry out an annual security review, providing an official report with the non-conformities that will be reported by ALEA to the Authorities.

XX.2. Permissions and access rights review

HR Department has the responsibility to provide to the Engineering Department a monthly report with all comers, leavers, and changes of roles during the previous month.

Each quarter, the Engineering Department organizes a manual review in all systems to make sure that permissions and accesses are updated, providing a report with the taken actions.

XX.3. Updates on gaming services

Critical gaming services are identified by the System Administration team of Engineering Department. Each month available updates will be manually checked by the System Administration team and when an update is stable, he or she will find the next best schedule, working in collaboration with the Product Department to apply the update.

If down time is expected, it will be communicated to the rest of the company and customers.

XXI. Social Media

Should ALEA make use of social media on the internet (Skype, Facebook, Twitter, etc.). This should only be done for business use and no confidential information should be disclosed over this medium. ALEA may decide at any time, to keep logs of chats and activities carried out using this medium.

XXII. Network & Remote Access

All ALEA employees, including service provider employees, may be granted a remote access (VPN):

- It is the responsibility of the employees, contractors, vendors, and agents with remote access privileges to the ALEA's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Company.
- Secure remote access must be strictly controlled and restricted from Company devices (MAC Filtered).
- All hosts that are connected to the Company internal networks via remote access technologies will be monitored on a regular basis.

With the exclusion of the "Guest WIFI", access to the ALEA network is strictly reserved to ALEA managed devices, unless otherwise approved by the ALEA management in writing.

XXIII. Vulnerability Management Policy

- ALEA should perform an independent vulnerability scan of its external network at least once a year ("web penetration test").
- ALEA should perform an independent vulnerability scan of its internal network at least once a year ("penetration test in situ").

- Regular vulnerability scans should be performed by the ALEA most critical systems exposed to the web, either by internal staff or a 3rd Party vendor (Casino + BO).
- For all findings or vulnerabilities identified during the tests carried out will be generated and documented sufficient evidence to prove the existence of the same. The format of the evidence can be variable in each case, screen capture, raw output of security tools, photographs, paper documents, etc.

XXIV. Incident Response Plan

Security incident means any incident (accidental, intentional, or deliberate) relating to the ALEA communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage your company.

The Incident response plan must be tested once annually. Copies of this incident response plan is to be made available to all relevant staff members and take steps to ensure that they understand it and what is expected of them:

- Employees of ALEA will be expected to report to the CTO or the maximum responsible of the Engineering Department for any security related issues.
- Each department must report an incident to the CTO (preferably) or to another member of the Engineering Department.
- The Engineering Department will investigate the incident and assist the potentially compromised department in limiting the exposure of sensitive data and in mitigating the risks associated with the incident.
- The Engineering Department will resolve the problem to the satisfaction of all parties involved, including reporting the incident to the regulator whenever appropriate.
- The Engineering Department will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.
- If an unauthorized access is identified or detected as part of the quarterly test, this should be immediately escalated to the CTO or a member of the Engineering Department that has the authority to stop, cease, shut down, and remove the offending device immediately.
- A department that reasonably believes it may have a leak of data, or a breach in any of the ALEA systems, must inform the CTO or the maximum responsible of the

Engineering Department. After being notified of a compromise, the Engineering Department will implement the Incident Response Plan.

The ALEA Security Incident Team is composed of:

- ✓ Eduard FUMÀS (CTO).
- ✓ Charlotte LECOMTE (CPO).
- ✓ Iñigo IGLESIAS (Head of DevOps).

XXV. Network Security

Firewall protection shall be put in place to safeguard the company against unauthorized intrusion attempts.

Wireless networks shall be password protected and used solely by the ALEA staff. Should guests wish to utilize an internet connection, a separate wireless connection shall be put in place, which is segregated from the ALEA network.

XXVI. Safeguarding of Equipment

Employees must sign for new equipment handed to them, so ALEA is in a better position to monitor and control the use of company equipment.

All workstations which are granted permission to access the environment will utilize the ALEA corporate endpoint security software (Including an anti-virus) which is deployed with every desktop/laptop build.

Servers and network devices will continually be monitored, and alerts will be sent in case of any detection or other unusual occurrences. The monitoring system will produce reports to review statistical information regarding server resource usage, any changes made to network and servers, as well as capacity planning.

All employees accessing the environment are locked down via the security policy and are informed of the access levels they are granted. The devices and servers are setup to be able to track employees' access to these devices as well as the policy to restrict user access to data as per security policy.

The Internet firewall protects the network from unauthorized access allowing only the necessary access to internal servers via its policy-based rule set.

To ensure and maintain security of applications, a unique identification is assigned to each person with access, to ensure that actions taken on critical data and systems can be traced to known and authorized users. All users will be required to be identified with a unique user ID (Corporate Id) before allowing them to access system components.

XXVII. Clear Desk Policy

Outside of regular working hours, all workers must clean their desks and working areas such that all sensitive or valuable data is properly secured.

XXVIII. Communication of Policies

ALEA shall ensure that employees read the Company's Policies and Procedures upon starting work with the Company and sign a compliance agreement for these Policies and Procedures.

XXIX. Right of Erasure & Right to Access

To complying with the regulation ALEA is subject to, the ALEA system shall be deemed to be auditable. As such, any activity performed on one of the ALEA systems can be recorded. This includes, but is not limited to, read, write, upload, download or share any document; Access or visit a portal (Such as Back-offices systems).

In compliance you can request access to that information:

- As an employee, following the procedure provided by the ALEA HR Department.
- As a 3rd Party, sending your request to the ALEA Product responsible (charlotte.lecomte@alea.com).

Similarly, but under the limits imposed by the compliance requirements (notably by the Malta IDPC), you may request such records to be deleted from the ALEA Systems.

XXX. Internal Audit

XXX.1. Introduction & Responsibility

ALEA monitors and traces significant actions of all employees that can direct or indirectly compromise the security or privacy of ALEA customers, employees, and systems.

The Engineering Department is responsible to know who acceded where, why, and when.

There are different thresholds define to detect abuse usages in ALEA systems informing immediately.

Data is kept in our systems for more than 2 years.

Each Manager will ensure the integrity and security of the files. It is also responsible to periodically check that no files have been destroyed or modified without their consent to safeguard the information.

XXX.2. Operational Internal Audit

At any time, the Internal Auditor can send an Internal Audit Invitation to the CTO with a list of requirements to assess the proper application of this Policy.

XXXI. JAMF (Mobile Device Management)

In recent years, mobile devices have become ubiquitous in enterprise use. Businesses and their workforces rely on mobile devices such as smartphones, tablets, and laptops for a wide assortment of tasks. And as working remotely has become essential, mobile devices have become an integral part of most organizations — vital tools for productivity and efficiency.

But because enterprise mobile devices access critical business data, they can threaten security if hacked, stolen, or lost. So, the importance of managing mobile devices has evolved such that IT and security leaders are now tasked to provision, manage and secure mobile devices within their respective corporate environments.

With a mature MDM platform, IT and Security departments can manage all of a company's devices, no matter their type or operating system. An effective MDM platform helps keep all devices secure while keeping the workforce flexible and productive.

Beyond managing device inventory and provisioning, MDM solutions protect the device's applications, data, and content. In this sense, MDM and mobile security are similar. However, MDM is a device-centric approach, whereas mobile security and unified endpoint management have evolved to a user-centric stance.

In an MDM program, employees can receive a dedicated work device, such as laptops or smartphones, or have a personal device remotely enrolled. Personal devices receive role-based access to enterprise data and email, a secure VPN, GPS tracking, password-protected applications, and other MDM software for optimal data security.

MDM software can then monitor the behaviors and business-critical data on enrolled devices. And with more sophisticated MDM solutions, they can be analyzed by machine learning and AI. These tools ensure devices are kept safe from malware and other cyberthreats. For example, a firm might assign a laptop or smartphone to a staff member or consultant, pre-programmed with a data profile, VPN and the other necessary software and applications. In this scenario, MDM offers the most control to the employer. With MDM tools, enterprises can track, monitor, troubleshoot and even wipe device data in the event of theft, loss, or a detected breach.

XXXI.1.1. Advantages of MDM

- **Device Tracking:** Each device enrolled with or issued by an enterprise can be configured to include GPS tracking and other programs. The programs allow an enterprise's IT professionals to monitor, update and troubleshoot the device in real time. They can also detect and report high-risk or non-compliant devices and even remotely lock or wipe a device if lost or stolen.
- **Mobile Management:** IT departments procure, deploy, manage, and support mobile devices for their workforce, such as troubleshooting device functionality. These departments ensure each device comes with the needed operating systems and applications for their users — including applications for productivity, security and data protection, backup, and restoration.
- **Application Security:** Application security can involve app wrapping, in which an IT administrator applies security or management features to an application. Then that application is re-deployed as a containerized program. These security features can determine whether user authentication is required to open an app; whether data from the app can be copied, pasted, or stored on the device; and whether the user can share a file.
- **Identity and access management (IAM):** Secure mobile management requires strong identity and access management (IAM). IAM allows an enterprise to manage user identities associated with a device. Each user's access within an organization

can be fully regulated, using such features as single sign-on (SSO), multifactor authentication and role-based access.

- **Endpoint security:** Endpoint security encompasses all devices that access a corporate network, including wearables, Internet of Things (IoT) sensors and non-traditional mobile devices. Endpoint security can include standard network security tools such as antivirus software and network access control and incident response, URL filtering and cloud security.

In ALEA, we have decided to integrate our company with JAMF.

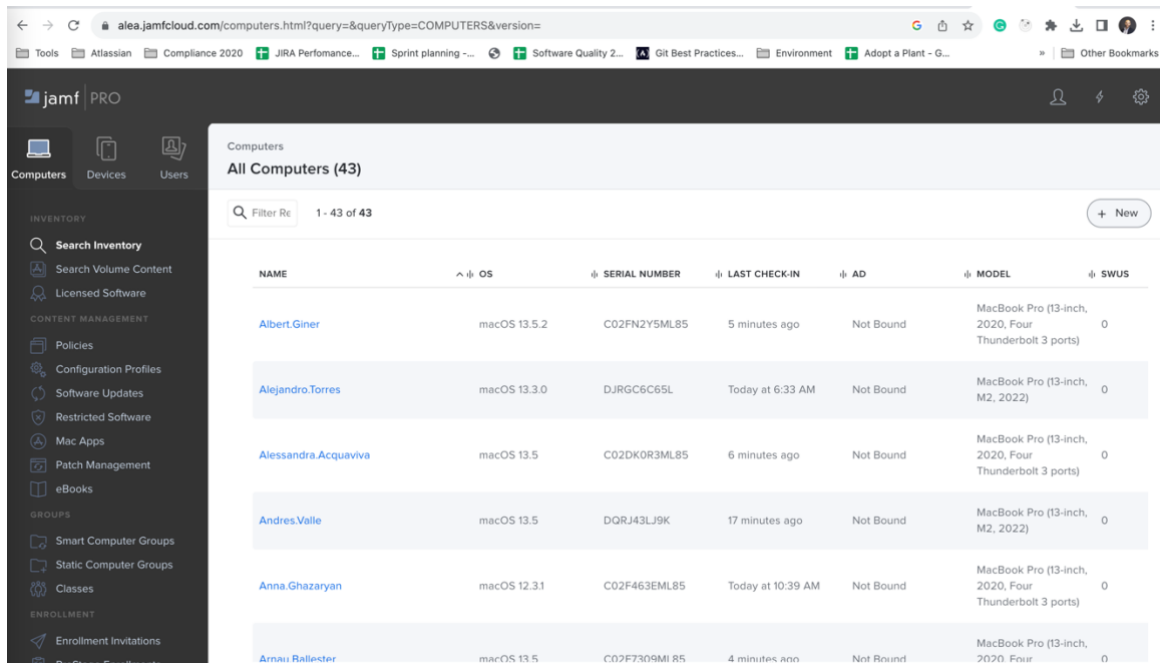
JAMF is a software and services company. Founded in 2002, it is now the industry leader in MDM (Mobile Device Management) for companies incorporating Apple devices into their business.

XXXI.1.2. Why JAMF?

The company focuses specifically on working with Apple products and maintains very close ties with its developers. In 2010, Apple became a JAMF customer. Two years later, sales of JAMF software were launched in all the corporation's retail shops. And in 2014, JAMF joined the Apple Mobility partnership programmer. Therefore, our first argument: it is safe to say that JAMF is up to date with all of Apple's innovative projects and developments.

From this comes another benefit: the timely update of all JAMF functions for the Apple operating system. As soon as a new version of the system is released – rest assured that all relevant changes will be immediately up to date and available on all your corporate devices. JAMF software also deserves your attention due to its scalable deployment, which requires no additional investment or time. IT staff can quickly and remotely configure all equipment, download the latest updates, and encrypt information, without having to worry about confidentiality.

JAMF has a relatively simple interface and extensive functionality to fully integrate devices into your business environment.



NAME	OS	SERIAL NUMBER	LAST CHECK-IN	AD	MODEL	SWUS
Albert Giner	macOS 13.5.2	C02FN2Y5ML85	5 minutes ago	Not Bound	MacBook Pro (13-inch, 2020, Four Thunderbolt 3 ports)	0
Alejandro Torres	macOS 13.3.0	DJRG6C65L	Today at 6:33 AM	Not Bound	MacBook Pro (13-inch, M2, 2022)	0
Alessandra Acquaviva	macOS 13.5	C02DK0R3ML85	6 minutes ago	Not Bound	MacBook Pro (13-inch, 2020, Four Thunderbolt 3 ports)	0
Andres Valle	macOS 13.5	DQRJ43LJ9K	17 minutes ago	Not Bound	MacBook Pro (13-inch, M2, 2022)	0
Anna Ghazaryan	macOS 12.3.1	C02F463EML85	Today at 10:39 AM	Not Bound	MacBook Pro (13-inch, 2020, Four Thunderbolt 3 ports)	0
Anna Rallester	macOS 13.5	C02F7309ML85	4 minutes ago	Not Bound	MacBook Pro (13-inch, 2020, Four Thunderbolt 3 ports)	0

XXXII.OKTA (Identity Management)

Okta is an identity management service that allows us to access any employer to any application on any device. It is hosted on a secure server. It makes use of cloud technologies to assist businesses to manage and securing user authentication into apps. It sells various services, including single sign-on, which is one of the greatest programs since it has the unique feature of allowing users to log in too many applications via a single centralized process. It is safe to use, and it protects our sensitive data even when others use our phones because it just takes minutes for developed technology to steal our personal information.

XXXII.1.2. Why OKTA?

Enterprises are searching for solutions to implement single sign-on (SSO) so that their employees can simply access all cloud and web apps without having to authenticate each one separately.

With the increasing diversity of devices, identification difficulties, security, employee mobility, vendor partnerships, and the exponential increase of unique application

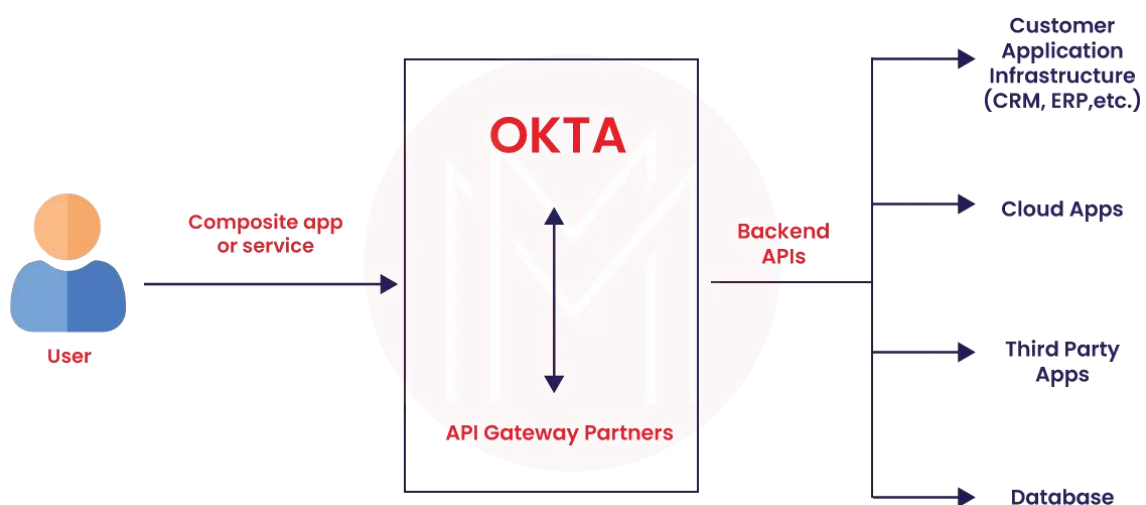
alternatives, businesses have faced new challenges as technology has developed and evolved.

Okta is a suitable identity cloud solution that bridges various on-premises apps for organizations that need an enterprise-grade identity management service developed for the cloud. It makes it easier for employees to use any program or device. Okta is built on a cloud infrastructure that is secure, dependable, and thoroughly audited, and it interfaces deeply with on-premises apps, directories, and identity management systems.

The increased use of remote working during the pandemic is highlighted by Okta's utility in Identity management and Access management-based services. The automated system is template-based and offers both identity and access management capabilities, making it simple to use. It also provides access management features, allowing you to integrate many apps. Okta is particularly beneficial to businesses that manage a big number of on-premises apps.

Consider your company's corporate network as a system that protects a variety of high-value digital assets, such as customer information, proprietary knowledge, and financial data. Every bit of information is vital, and every device linked to your network poses a security risk. With remote work becoming more widespread, it's not uncommon for employees to log in too many accounts, and many of them use passwords like abc123 or qwerty that they've used before.

Enterprise-level workplace identity management software, such as Okta, is the solution to this issue. It not only improves network security, but it also cuts down on the time your IT department spends on password requests.



Okta offers identity and access management (IAM) solutions for both businesses and individuals. Okta's web-based single sign-on (SSO) program is used by businesses to provide a centralized interface for accessing third-party systems. Okta enables employees to gain safe access to popular cloud programs like Gmail, Office 365, Salesforce, and the multitude of other apps they need to conduct their jobs.

Okta is platform-agnostic, allowing users from any organization to access linked SSO accounts using a web-based dashboard, browser extensions, and mobile apps. There are various advantages to using Okta, including:

- Management of the entire life cycle
- The world's largest directory
- Access control for application programming interfaces (APIs)
- Provisioning of users is done automatically.

Okta has a proven track record as one of the first entrants in the IAM (Identity Access Management) field. SSO login is enabled for every app your users need to access during their workday thanks to the solution's numerous integration options.

Delegated authentication, provisioning and de-provisioning, directory sync, and AD password management are all supported by Okta's cloud platform, which offers 99.99 percent availability and zero planned downtime. Changes in Active Directory or Okta's direction are synchronized incrementally.

Employees, partners, and customers all have continuous access to business-critical apps. Because the system requires little customization and has a low license management cost, it can save businesses up to 60% on the total cost of ownership.

XXXII.1.2. OKTA Features

The Okta solution arose from the specific challenges of how technology has evolved and moved in the face of increasing device variety, identity issues, security, workforce mobility, vendor partnerships, and the exponential expansion of unique application alternatives.

Provisioning, Single Sign-On (SSO), Active Directory (AD) and LDAP integration, centralised user de-provisioning, multifactor authentication (MFA), mobile identity

management, and configurable rules for corporate security and control are just a few of Okta's capabilities.

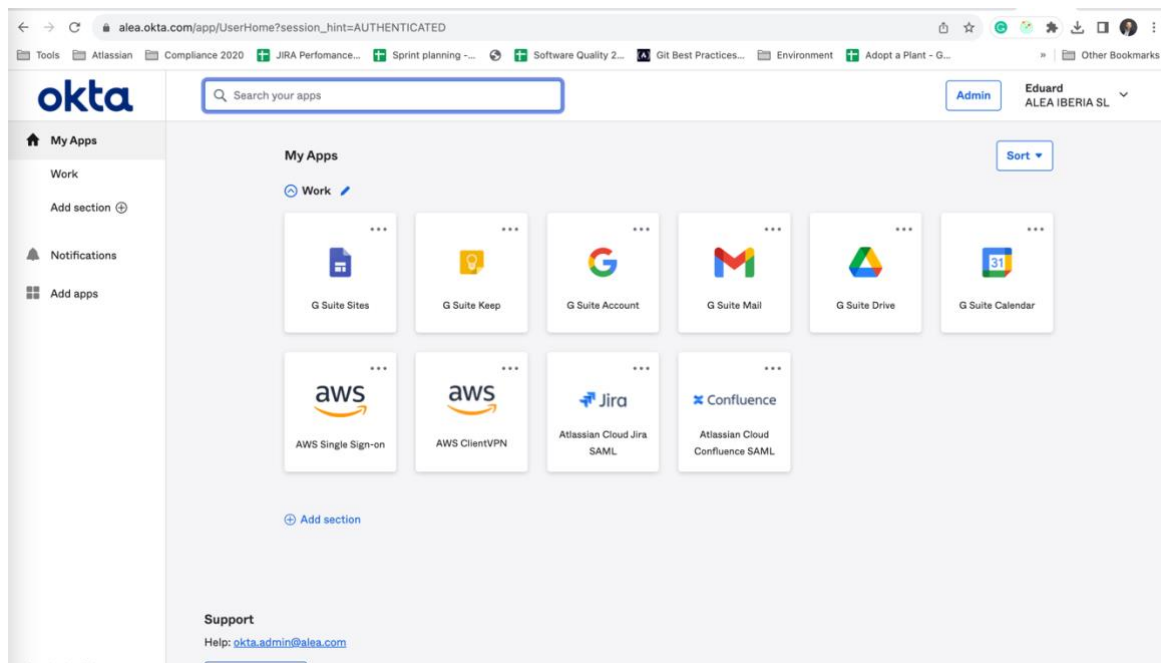
The Okta Integration Network, a network of pre-integrated applications, brings all these features together (OIN). The OIN offers a variety of integration possibilities, including single sign-on (SSO) for all the apps your employees use daily.

XXXII.1.3. Benefits of using OKTA?

- Okta helps us save time, which is quite valuable.
- It is available at an affordable price, so it saves our money; many organizations want to use the best applications, but due to cost, they compromise and use other applications at a lower price; however, Okta never disappoints any type of organization; it is available for all small to globalized organizations, and it is even affordable for small businesses, so it saves our money.
- Some programs function similarly to a toolkit. They simply grant access to our users and applications, which takes time and causes delays in work, while Okta integrated our applications, saving time and resources.
- It maintains our authentication, preventing unauthorized access and allowing only those users who have been verified. It safeguards our sensitive and personal information, as well as that of our users. It safeguards our computers by adhering to a set of flexible policies.
- It allows users to log in to all applications at once with a single password, rather than having to remember several passwords. Remembering multiple passwords can be difficult, and we may become confused and forget them, but with Okta, we only need single passwords for all applications. Single sign-on for all applications at once is easier to remember than many passwords, and it is also secure because it is your personal information that only you have access to.

Information Security Policy

Version 2.5



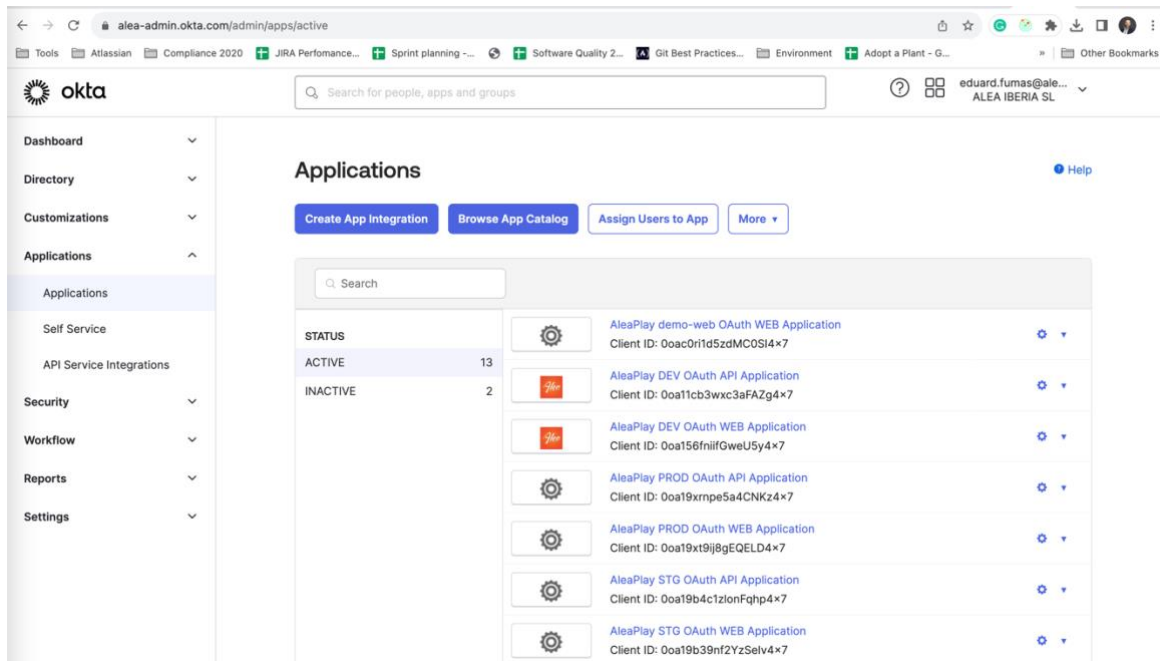
XXXIII. Safeguarding of Applications

ALEA is based on Microservices Architecture. So, we are using different safeguarding depending on each application.

XXXIII.1. CMS

XXXIII.1.1. Introduction

In this application, we are using OKTA Java Library as an SSO.

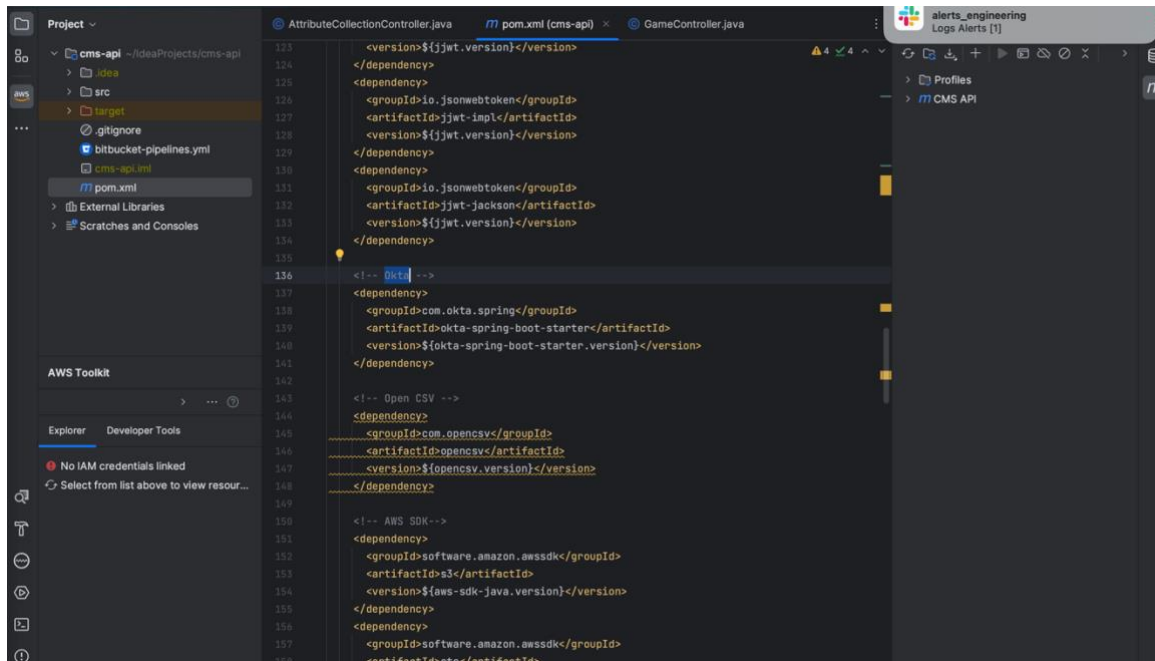


In this image, we can see that the OKTA Applications allow these domains to access:

- <https://cms.dev.aleaplay.com>: Development Environment
- <https://cms.stg.aleaplay.com>: Staging Environment
- <https://cms.aleaplay.com>: PROD Environment

XXXIII.1.2. How it Works?

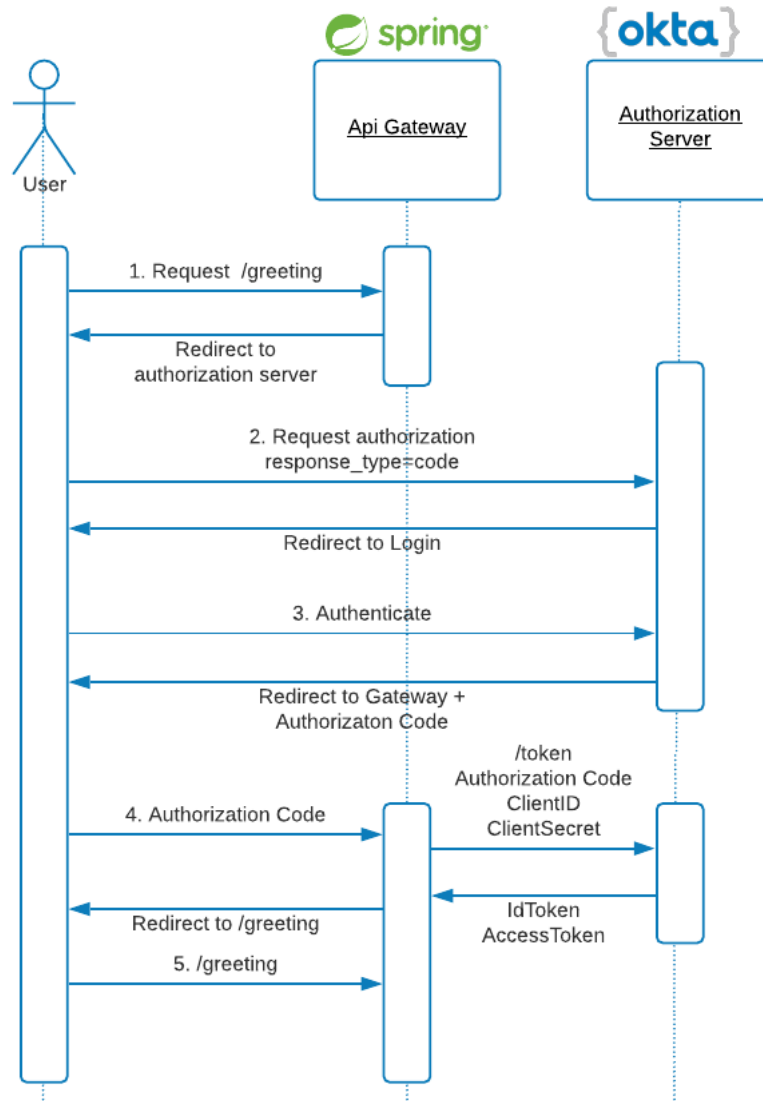
With Spring Starter for OKTA, now you can get started quickly to build the authentication workflow for a web application that uses OKTA AD and OAuth 2.0 to secure its back end. It also enables developers to create a role based authorization workflow for a Web API secured by OKTA AD, with the power of the Spring Security Filter Chain.



XXXIII.1.3. Implementation

This package provides 2 ways to integrate with Spring Security and authenticate with OKTA Active Directory.

- Authenticate in backend, auto configuration for common OKTA Active Directory OAuth2 properties and OAuth2UserService to map authorities are provided.
- Authenticate in frontend, sends bearer authorization code to backend, in backend a Spring Security filter validates the JWT token from OKTA AD and save authentication. The JWT token is also used to acquire a On-Behalf-Of token for OKTA AD Graph API so that authenticated user's membership information is available for authorization of access of API resources. Below is a diagram that shows the layers and typical flow for Single Page Application with Spring Boot web API backend that uses the filter for Authentication and Authorization.



The authorization flow is composed of 3 phrases:

- Login with credentials and validate id_token from OKTA AD
- Get On-Behalf-Of token and membership info from OKTA AD Graph API
- Evaluate the permission based on membership info to grant or deny access

To see more information about [OKTA + Spring Boot](#)

XXXIII.2. Launch-API & Customer-API

To manage the security of this application, we are using JSON Web Token (JWT) + a custom Signature Header.

XXXI.2.1. What is JSON Web Token?

JSON Web Token (JWT) is an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the **HMAC** algorithm) or a public/private key pair using **RSA** or **ECDSA**.

Although JWTs can be encrypted to also provide secrecy between parties, we will focus on *signed* tokens. Signed tokens can verify the *integrity* of the claims contained within it, while encrypted tokens *hide* those claims from other parties. When tokens are signed using public/private key pairs, the signature also certifies that only the party holding the private key is the one that signed it.

XXXI.2.2. Why are we using JSON Web Token?

- **Authorization:** This is the most common scenario for using JWT. Once the user is logged in, each subsequent request will include the JWT, allowing the user to access routes, services, and resources that are permitted with that token. Single Sign On is a feature that widely uses JWT nowadays, because of its small overhead and its ability to be easily used across different domains.
- **Information Exchange:** JSON Web Tokens are a good way of securely transmitting information between parties. Because JWTs can be signed—for example, using public/private key pairs—you can be sure the senders are who they say they are. Additionally, as the signature is calculated using the header and the payload, you can also verify that the content hasn't been tampered with.

To see more information about JWT: <https://jwt.io/introduction/>

XXXI.2.3. Custom Signature Header

The signature is meant to ensure that the sensitive parameters of a game launch request haven't been altered. It must be generated on server-side by the casino and passed as parameter of the initialization of a Game Launcher Object (GLO).

It must be generated using the secret ApiKey provided during the integration kick-off.

It must be generated as follows:

SHA512(casinoPlayerId + casinoSessionId + country + currency + secretApiKey)

XXXIII.3. Transaction-API

XXXI.3.1. Introduction

To manage the safeguarding of these applications we are using Amazon Web Application Firewall (AWS WAF).

AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns you define. You can get started quickly using Managed Rules for AWS WAF, a pre-configured set of rules managed by AWS or AWS Marketplace Sellers. The Managed Rules for WAF address issues like the OWASP Top 10 security risks. These rules are regularly updated as new issues emerge. AWS WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of security rules.

With AWS WAF, you pay only for what you use. The pricing is based on how many rules you deploy and how many web requests your application receives. There are no upfront commitments.

You can deploy AWS WAF on Amazon CloudFront as part of your CDN solution, the Application Load Balancer that fronts your web servers or origin servers running on EC2, or Amazon API Gateway for your APIs.

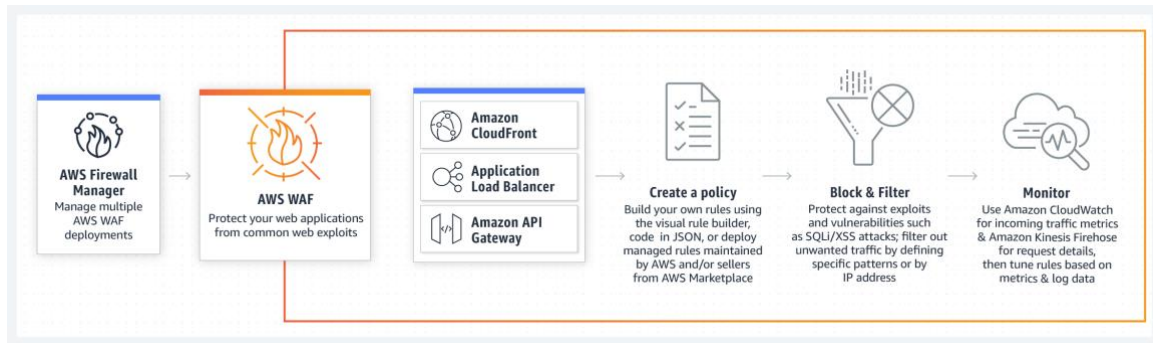
The benefits of using AWS WAF are:

- Agile protection against web attacks
- Save time with managed rules.
- Improved Web Traffic visibility
- Ease of deployment & maintenance
- Cost effective web application protection.
- Security integrated with how we develop applications.

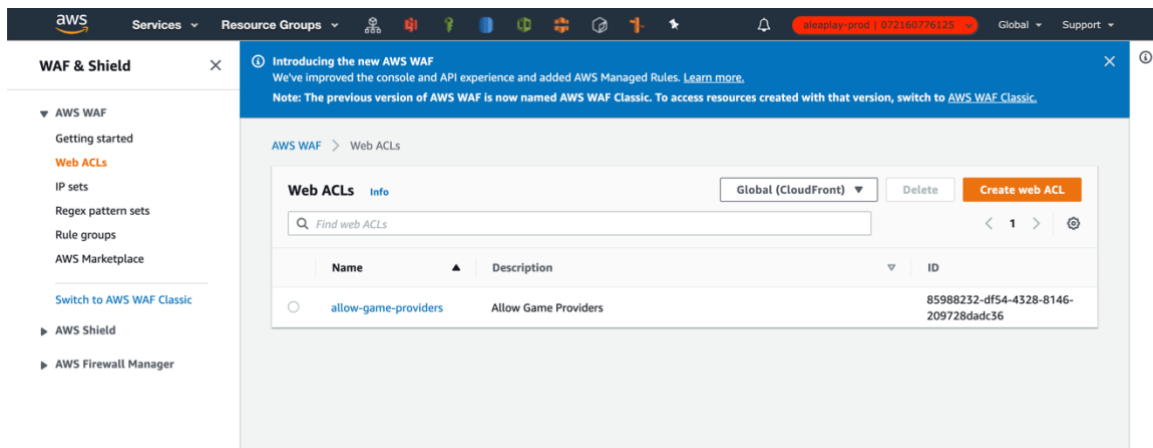
Information Security Policy

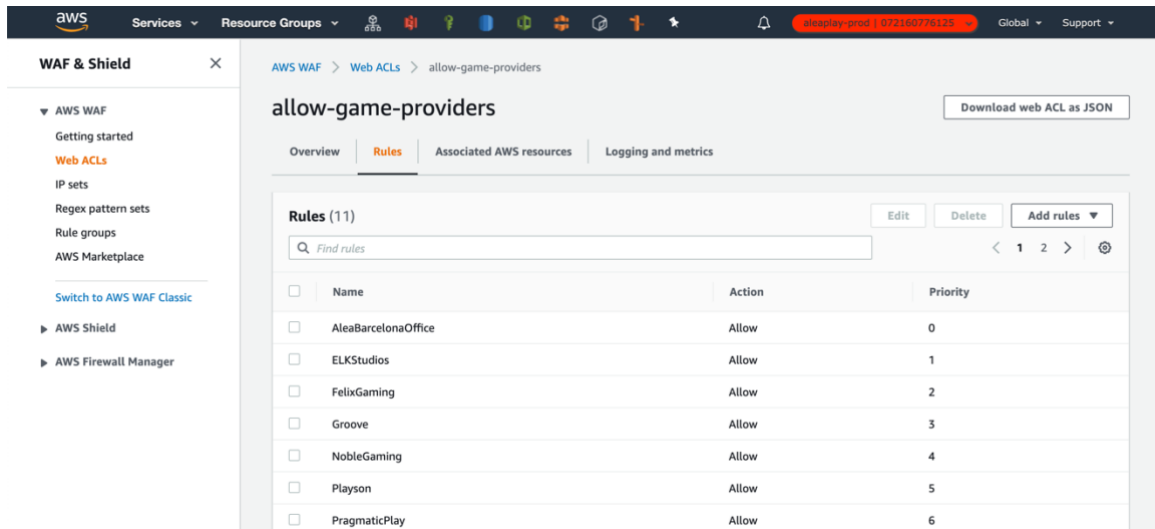
Version 2.5

XXXI.3.2. How it works?



In the following images, we can see the configuration of our AWS WAF on Production:





XXXIV. Back-end automatic log-off

XXXIV.1. Introduction

As we mentioned before, we are using OKTA Active Directory to manage the access in our Backend.

When a user authenticates with OKTA AD, a single sign-on session (SSO) is established with the user's browser and OKTA AD. The SSO token, in the form of a cookie, represents this session. The SSO session token is not bound to a specific resource/client application. SSO session tokens can be revoked, and their validity is checked every time they are used.

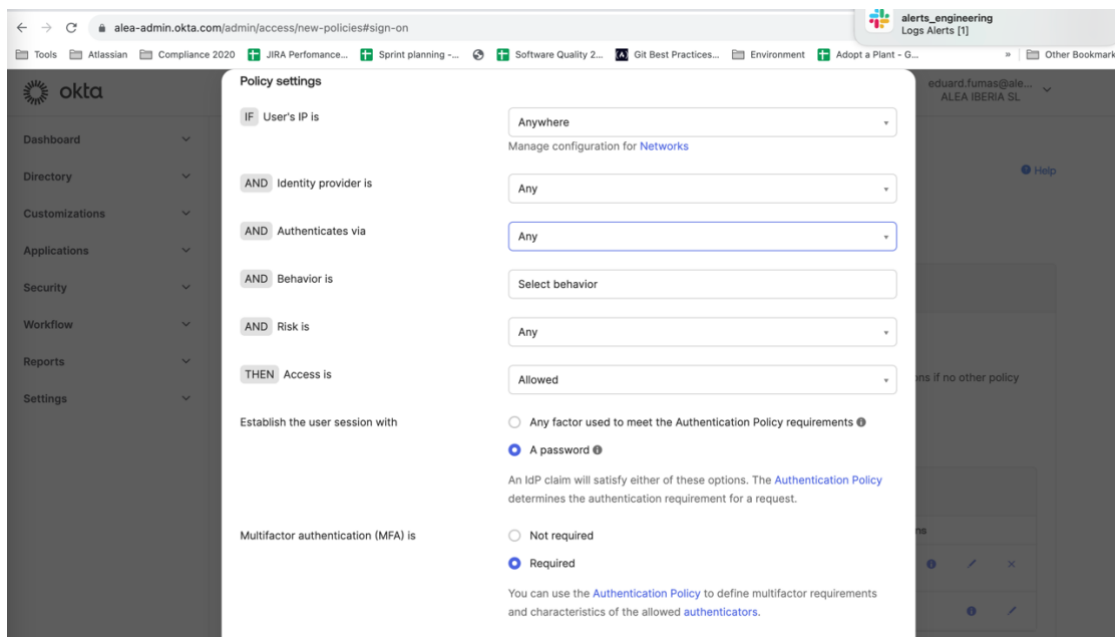
OKTA AD uses two kinds of SSO session tokens: persistent and nonpersistent. Persistent session tokens are stored as persistent cookies by the browser. Nonpersistent session tokens are stored as session cookies. (Session cookies are destroyed when the browser is closed.) Usually, a nonpersistent session token is stored. But, when the user selects the **Keep me signed in** check box during authentication, a persistent session token is stored.

Nonpersistent session tokens have a lifetime of **24 hours**. Persistent tokens have a lifetime of 180 days. Anytime an SSO session token is used within its validity period, the validity period is extended another 24 hours or 180 days, depending on the token type. If an SSO session token is not used within its validity period, it is considered expired and is no longer accepted.

You can use a policy to set the time after the first session token was issued beyond which the session token is no longer accepted. (To do this, use the Session Token Max Age property.) You can adjust the lifetime of a session token to control when and how often a user is required to re-enter credentials, instead of being silently authenticated, when using a web application.

XXXIV.2. Token lifetime policy properties

A token lifetime policy is a type of policy object that contains token lifetime rules. Use the properties of the policy to control specified token lifetimes. If no policy is set, the system enforces the default lifetime value.



The screenshot shows the Okta admin console at the URL `alea-admin.okta.com/admin/access/new-policies#sign-on`. The left sidebar contains navigation links: Dashboard, Directory, Customizations, Applications, Security, Workflow, Reports, and Settings. The main content area is titled "Policy settings" and displays a configuration form for a new policy.

The form includes the following sections:

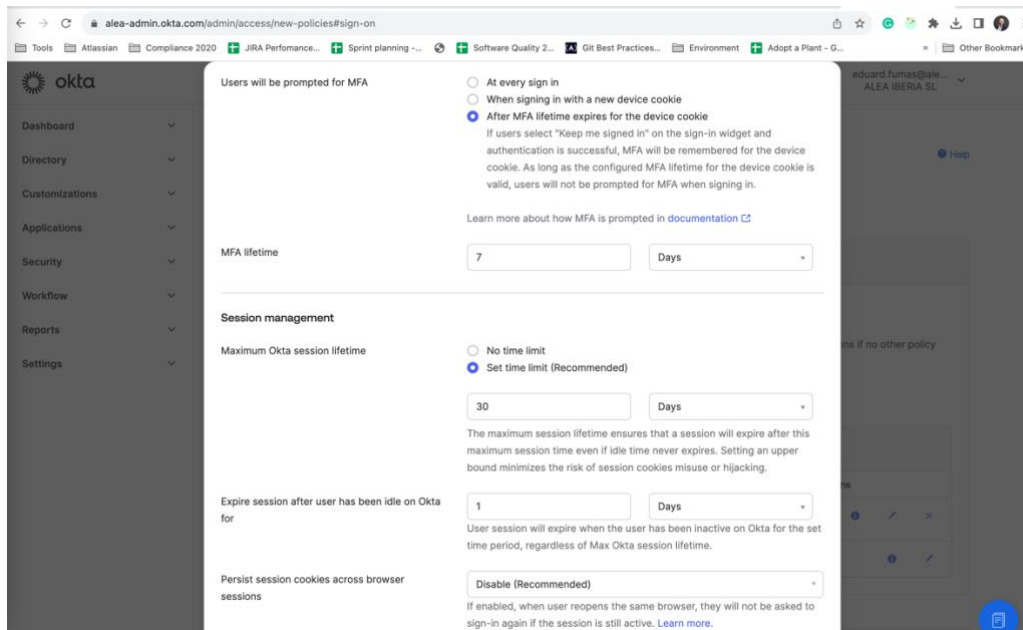
- IF** (Conditions):
 - User's IP is: `Anywhere` (dropdown)
 - AND** Identity provider is: `Any` (dropdown)
 - AND** Authenticates via: `Any` (dropdown)
 - AND** Behavior is: `Select behavior` (dropdown)
 - AND** Risk is: `Any` (dropdown)
 - THEN** Access is: `Allowed` (dropdown)
- Establish the user session with**:
 - ☐ Any factor used to meet the Authentication Policy requirements
 - ☒ A password

An IdP claim will satisfy either of these options. The [Authentication Policy](#) determines the authentication requirement for a request.
- Multifactor authentication (MFA) is**:
 - ☐ Not required
 - ☒ Required

You can use the [Authentication Policy](#) to define multifactor requirements and characteristics of the allowed [authenticators](#).

Information Security Policy

Version 2.5



Information Security Policy

Version 2.5

Property	Policy property string	Affects	Default	Minimum	Maximum
Access Token Lifetime	AccessTokenLifetime ²	Access tokens, ID tokens, SAML2 tokens	1 hour	10 minutes	1 day
Refresh Token Max Inactive Time	MaxInactiveTime	Refresh tokens	90 days	10 minutes	90 days
Single-Factor Refresh Token Max Age	MaxAgeSingleFactor	Refresh tokens (for any users)	Until-revoked	10 minutes	Until-revoked ¹
Multi-Factor Refresh Token Max Age	MaxAgeMultiFactor	Refresh tokens (for any users)	Until-revoked	10 minutes	Until-revoked ¹
Single-Factor Session Token Max Age	MaxAgeSessionSingleFactor	Session tokens (persistent and nonpersistent)	Until-revoked	10 minutes	Until-revoked ¹
Multi-Factor Session Token Max Age	MaxAgeSessionMultiFactor	Session tokens (persistent and nonpersistent)	Until-revoked	10 minutes	Until-revoked ¹

- ¹365 days is the maximum explicit length that can be set for these attributes.
- ²To ensure the Microsoft Teams Web client works, it is recommended to keep AccessTokenLifetime to greater than 15 minutes for Microsoft Teams.