Axidian

WHITE PAPER

Axidian Access

Centralized User Authentication and Access Control

Table of contents

Reliable Authentication and Centralized Access Management

Protecting access to corporate resources is one of the key tasks of a company's information security strategy. Critical components in addressing this task are reliable user authentication and centralized access management.

The choice of a **reliable authentication technology** depends on several factors:

- **Applicability** — User scenarios can significantly limit the selection of authentication technologies. For instance, most remote access scenarios make it impractical to use authentication devices that need to be physically connected to the user's workstation.
- **Security** — How well the authentication technology meets the organization's information security requirements. For example, one-time passwords (OTPs) offer an adequate level of protection for most remote scenarios. However, organizations may be required to implement other technologies to comply with external regulations or industry standards.
- **Convenience** — How comfortable the technology is for end users in their work environment. For example, accessing a desktop using OTPs may be inconvenient, as it requires generating and entering a password multiple times during the workday.
- **Cost of use** — This includes several components: implementation costs, the ability to reuse existing authentication devices, total cost of ownership, and the complexity of integrating the authentication technology with target information systems.

Centralized Access Management

Employees have access to a wide range of information systems, which are managed by different groups of administrators (such as Active Directory, databases, and application systems). Managing such access requires a specialized centralized solution that enables:

- Consolidation of information about the systems accessible to each user in a single location
- Implementation of a Single Sign-On (SSO) mechanism
- Specification of the authentication technologies required for access to each information system
- Denial of access to specific information systems
- Logging of employee access events

Centralization is achieved through the use of various user authentication technologies and integration protocols, depending on what the target system supports. Due to the vast diversity of applications and technologies they employ, a universal integration mechanism does not exist. Therefore, it is essential that the access management system supports multiple mechanisms and protocols for integration with target applications. This ensures coverage of the maximum number of information systems.

Axidian Access

Axidian Access is a platform designed to build a centralized system for managing user access to a company's information resources.

Axidian Access enables the use of strong and multi-factor user authentication technologies when accessing information resources. These technologies reduce information security risks by supplementing or replacing passwords. A variety of authentication methods are supported, allowing Axidian Access to adapt to specific access scenarios and offer users the most suitable authentication technology for each case.

In addition to diverse authentication technologies, Axidian Access employs a wide range of integration technologies that enable the connection of target applications to the authentication system. These include implementations of the Single Sign-On approach (both Web and Enterprise SSO), standardized authentication protocols, and agent modules.

Axidian Access provides controlled access to information resources from both the company's internal network and externally accessible systems such as email, VPN, VDI, PAM, and web portals. This approach enables the creation of a centralized access provisioning system that covers all target systems in use, minimizes user requests to the help desk, reduces infrastructure maintenance costs, and improves user productivity.

Axidian Access Platform

The foundation of the platform is a set of core modules that implement the business logic of the system and ensure the operation of the server infrastructure and management tools (see Figure 1).

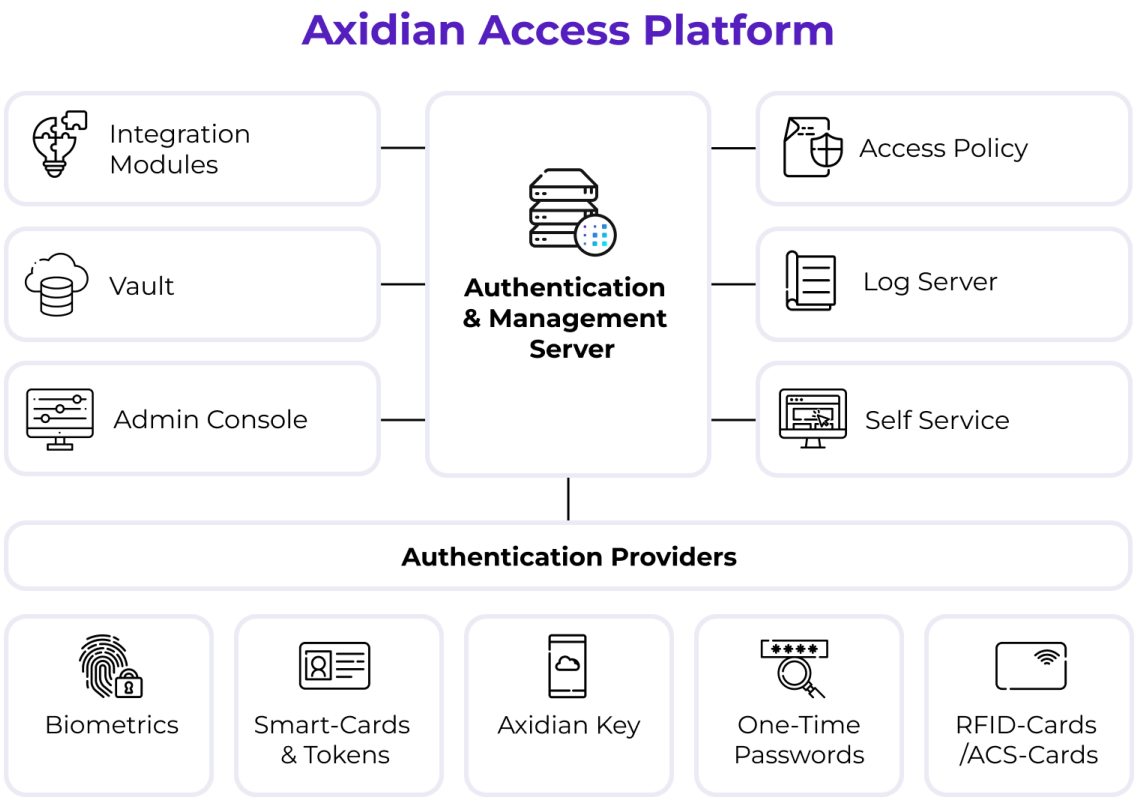

Figure 1. Axidian Access Platform

The core modules of Axidian Access include:

Axidian Access Authentication and Management Server (Core Server).

This server is the core of the system and powers the entire platform. It handles user authentication and implements the business logic of the solution. The server is a .NET application and supports clustered deployment, enabling high performance and fault tolerance regardless of implementation scale. It can be installed on devices running Linux or Windows.

Data Storage.

All system data is stored in a unified SQL repository accessed only by the Core Server. Data storage and exchange with the server are encrypted.

Event Log.

All events related to configuration changes and access attempts are recorded in a unified log hosted on a dedicated server. The log can be stored in Windows Event Log format or in Axidian Access's own format within an SQL DBMS. Additionally, events can be sent to an external log via the Syslog protocol for integration with SIEM systems.

Management Console.

Delivered as a web application, the console allows AM administrators to view and modify system parameters, policies, applications, user and device settings, and review the system event log.

User Console.

Enables users to register or update their authentication credentials (such as push authenticators and OTP generators), view login history, and release their device from Exchange quarantine.

Authentication Providers:

These allow Axidian Access to work with various user authentication technologies. A provider offers a unified interface for the system to perform operations with specific authentication technologies: collecting and validating user credentials.

Axidian Access supports the following authentication technologies:

- Cryptographic smart cards and USB tokens
- Contactless RFID cards (used in physical access control systems), including EM-Marin, HID iClass, HID Proximity, and Mifare formats
- Hardware and software tokens for generating one-time passwords using OATH protocols: TOTP and HOTP
- One-time codes sent via SMS, Email, or Telegram
- Out-of-band authentication and push notifications using the **Axidian Key mobile app**. Axidian Key is available for iOS, Android, and HarmonyOS. Users confirm login operations within the smartphone app, where operation details are shown so they can verify the target system. Axidian Key also supports OTP generation via the TOTP protocol.
- OTP delivery through any external module or script, enabling integration with the company's internal messaging systems (Axidian Access Messages Proxy).

These technologies can be combined to implement **multi-factor authentication (MFA)**.

Other important components of the Axidian Access system include access policies and roles:

Access Policies define the rules for access, specifying which authentication technologies are to be used for which applications, and setting the scope of operator and administrator permissions.

Roles define privileges for working in the Axidian Access Management Console. There are three roles:

- **Administrator** — full access to all functions and settings
- **Operator** — permission to work with system users
- **Inspector** — read-only access

Role-based rights can be assigned system-wide or within specific policy scopes.

Integration Modules

Each integration module can be used independently and is designed to address specific tasks related to access protection and user authentication within particular applications. The modules are designed to work together, enabling the creation of any configuration for the authentication system, and allowing it to be adapted to the current needs and IT landscape of the organization (see Figure 2).

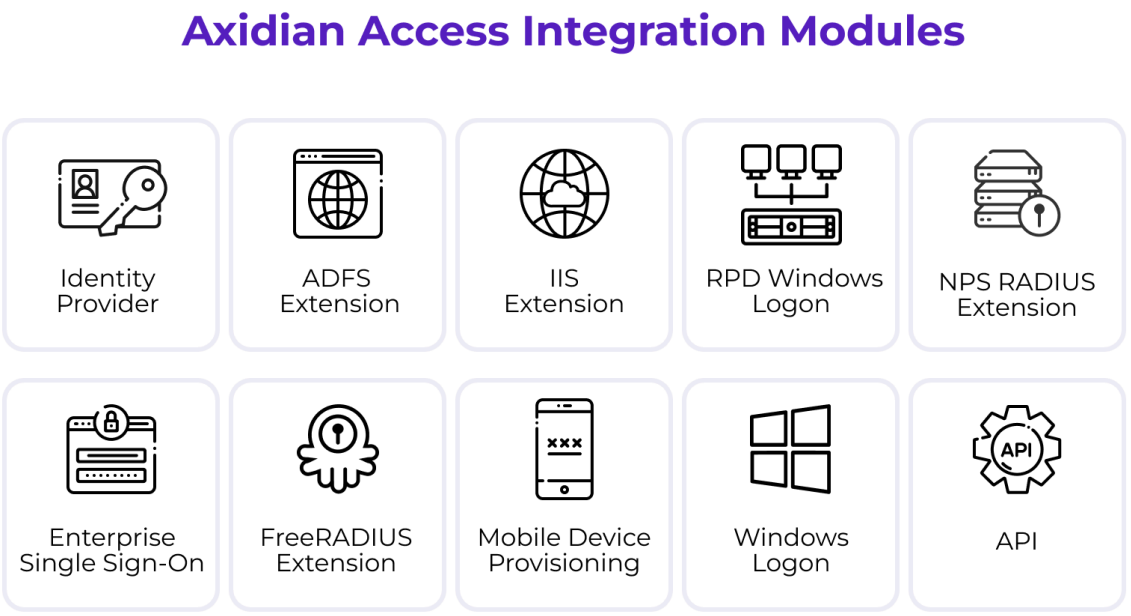

Figure 2. Axidian Access Integration Modules

The Axidian Access software suite includes the following integration modules for target information systems:

Axidian Access Identity Provider

The Axidian Access Identity Provider (IDP) module is used to enable multi-factor authentication and seamless access to web applications (Web Single Sign-On, or WebSSO). To integrate with target systems, this module supports the following protocols:

- SAML 2.0 (Security Assertion Markup Language);
- OIDC 1.0 (OpenID Connect);
- OAuth 2.0.

This ensures compatibility with a wide range of commercial systems. The use of Axidian Access IDP eliminates the need for users to remember multiple credentials: a single set of credentials provides access to all integrated systems. Authentication is performed centrally on the Identity Provider side.

Axidian Access IDP is implemented as a web application and is deployed within the customer's infrastructure. When accessing a target application, the user is redirected to the IDP page for authentication. Upon successful authentication, the user is redirected back to the target application with an "authenticated" status, and their session begins.

Integration is performed server-side, enabling MFA and WebSSO authentication on any device with a browser: PC, smartphone, or tablet.

Axidian Access IDP supports the following user authentication technologies in any combination: domain password, one-time passwords using OATH TOTP and HOTP, one-time codes via SMS, email, and Telegram, and out-of-band authentication using the **Axidian Key** mobile app.

Axidian Access Windows Logon

Axidian Access Windows Logon enables secure access to the Windows operating system using strong authentication technologies in a Microsoft Active Directory environment. To facilitate this, a Windows Logon agent is installed on user workstations. The agent installer is implemented as a standard MSI package (Microsoft Windows Installer), allowing for quick and large-scale deployment and updates via tools such as Active Directory Group Policies, Microsoft System Center Configuration Manager (SCCM), and others.

Integration with the Windows operating system is done through the standard Credentials Provider mechanism, which allows third-party developers to integrate their own authentication technologies into the Windows login interface. This mechanism supports not only logging into Windows using Axidian Access, but also authenticating within the OS itself — for example, when accessing domain resources, web applications, and more.

Windows Logon supports all authentication technologies available in Axidian Access, including smart cards, RFID cards, OTPs, and others.

Offline Mode

To improve resilience, Windows Logon can create a local cache on the user's PC. This cache contains authentication data and is used when there is no connection to the server infrastructure (offline mode), such as during a network outage or while traveling. The lifetime of the local cache can be restricted by a number of days or a calendar date. A cache is created only for users explicitly authorized by the Axidian Access administrator. Windows Data Protection API is used to safeguard local data.

Active Directory User Password Management

Axidian Access does not replace the native Active Directory authentication system, but instead automates user password management. In this configuration, password-based authentication becomes an internal mechanism used solely at the software level.

An Axidian Access administrator can configure the system so that, upon registration of a user's first authenticator, their password is automatically changed to a random value. This value is not disclosed to either the user or the system administrator. As a result, domain access becomes

possible only through Windows Logon.

Subsequently, the user's password is updated automatically — either in response to an operating system request or based on a predefined schedule.

Axidian Access RDP Windows Logon

The Axidian Access RDP Windows Logon module is used to implement two-factor authentication for connections via the Remote Desktop Protocol (RDP). In this setup, the first factor is the domain password, and the second factor is either a one-time password (OTP) or login confirmation via the Axidian Key mobile app.

The OTP can be:

- Generated by the user on their smartphone using an app
- Produced by a dedicated hardware token (OTP token)
- Delivered via SMS, Email, or Telegram

RDP Windows Logon should be installed on the destination terminal server where the user logs in. No components need to be installed on the client PC. The solution also supports:

- Operation in conjunction with Remote Desktop Gateway
- Connections using non-standard ports.

Axidian Access Enterprise Single Sign-On (Enterprise SSO)

Axidian Access Enterprise Single Sign-On (Enterprise SSO) implements a single sign-on approach for legacy applications that do not support native SSO mechanisms. The system centrally stores user passwords for all applications that require credential input and automatically inserts them into login forms as needed.

Enterprise SSO can be applied to any type of application — Windows, Java, web, .NET — regardless of architecture: single-tier, two-tier, three-tier, "thick" clients, "thin" clients, or terminal applications.

This technology frees employees from:

- Remembering and securely storing passwords
- Manually entering passwords
- Periodically changing passwords according to security policies

To enable this functionality, an Enterprise SSO agent is installed on the user's workstation. This agent monitors application launches and intercepts authentication forms when they appear on screen. It also includes extensions for popular browsers — Internet Explorer, Google Chrome, Mozilla Firefox, and Microsoft Edge — enabling seamless work with web applications.

Enterprise SSO Integration with Target Systems

Enterprise SSO can be configured to work with an application without requiring any modifications to the application's server-side or client-side code.

Supporting a new application involves creating a special XML-format template, implemented in Axidian Access Enterprise SSO's internal scripting language. This language allows developers to specify which application forms should trigger a response.

Enterprise SSO's response may include:

- Re-authenticating the user with strong authentication
- Filling in login form fields (e.g., username, password)
- Clicking required interface elements (e.g., the "Login" button)
- Logging the event in the audit journal.

Password Change in the Target Application

To minimize information security risks, most information systems allow or require users to change their password either after the first login or when the password expires.

Enterprise SSO handles this scenario by automatically managing the password change process, transparently to the user. It temporarily blocks the user's access to the password change window, generates a new password, populates the fields for "new password" and "confirmation," and clicks the "OK" button.

Once the target system confirms that the password change was successful, the Enterprise SSO agent stores the new password in the Axidian Access database. From that point forward, neither the user nor the administrator knows the new password, and therefore cannot access the target system bypassing Enterprise SSO.

This capability to handle password changes is only available if the ESSO template for the application supports a reaction to the appearance of such a window.

Support for Terminal Execution Environments

Axidian Access Enterprise SSO is adapted for use in terminal environments, which allows employees to avoid directly using their passwords when working with applications inside a terminal session. For this, the Enterprise SSO agent must be installed on the terminal server.

In certain situations — such as when accessing highly sensitive applications — the employee may be required to undergo an additional authentication step. If the authentication technology involves external hardware connected to the employee's PC (for example, a fingerprint scanner), communication is established between the Enterprise SSO agent on the terminal server and the external device.

Enterprise SSO communicates via Microsoft RDP protocols, meaning that no additional software needs to be installed on the employee's PC — aside from the necessary drivers and runtime libraries required for the hardware to function.

Axidian Access ADFS Extension

Web applications hosted on Internet Information Services (IIS) can be integrated with the Axidian Access software suite using the ADFS mechanism and the Axidian Access ADFS Extension component.

The ADFS Extension acts as a multi-factor authentication (MFA) provider for the Microsoft ADFS server, adding a second authentication factor to the access process. This approach allows integration with target applications without modifying them: when a user attempts to log in, they are redirected to an ADFS authentication web page, where the Axidian Access ADFS Extension prompts them for the second factor. Upon successful authentication, the user is redirected back to the target application.

ADFS technology is supported by Microsoft web applications such as:

- Outlook Web Access
- SharePoint
- Skype for Business
- Office 365
- And others

As the second factor, Axidian Access ADFS Extension supports:

- One-time passwords using OATH, TOTP, and HOTP
- OTPs delivered via SMS, Email, and Telegram
- Out-of-band authentication using the Axidian Key mobile application.

Axidian Access IIS Extension

Axidian Access IIS Extension is a specialized integration module for web applications running on Internet Information Services (IIS) that do not support the ADFS mechanism.

This module is installed on the web server hosting the target application and enables two-factor authentication without requiring any changes to the application's source code. The module intercepts authentication attempts: after entering a username and password, the user is redirected to a separate page to enter a one-time password (OTP).

The module also supports single-factor authentication mode. This is particularly useful for applications such as Exchange ActiveSync (EAS), where the domain password can be excluded from the authentication scheme. Instead, an application-specific password — used only for EAS — is entered by the user in their mobile client to access corporate email.

IIS Extension can be used with any IIS-based web applications, such as:

- Outlook Web Access
- RD Web Access
- Exchange ActiveSync
- And others

Axidian Access NPS RADIUS Extension

The Axidian Access NPS RADIUS Extension is a plugin module for Microsoft Network Policy Server (NPS), which is part of Windows Server. It enables two-factor authentication for RADIUS-compatible services and applications. To implement this, the following steps are required:

1. Deploy an NPS server within the enterprise network to enable RADIUS protocol-based authentication using user credentials from the Active Directory directory.
2. Configure the target application to authenticate users via RADIUS through the NPS server.
3. Install the Axidian Access NPS RADIUS Extension on the NPS server. This extension processes authentication requests and prompts the user for a second authentication factor.

The second factor authentication is performed by the Axidian Access server, and the result is relayed back to the target application via the NPS server.

Axidian Access NPS RADIUS Extension supports the following second-factor authentication methods:

- One-time passwords via OATH TOTP and HOTP
- OTP codes sent through SMS, Email, and Telegram
- Out-of-band authentication using the Axidian Key mobile application

RADIUS authentication can be applied in a wide range of VPN, VDI, and PAM solutions, including those from Cisco, Citrix, Check Point, and VMware.

Axidian Access FreeRADIUS Extension

The Axidian FreeRADIUS Extension is a module designed to implement two-factor authentication for RADIUS-compatible services and applications.

As a second authentication factor, the Axidian FreeRADIUS Extension supports:

- One-time passwords using OATH TOTP and HOTP
- OTP codes delivered via SMS
- User-defined passwords
- Out-of-band authentication using the Axidian Key mobile application

Axidian Access Mobile Device Provisioning

Axidian Access MDP is a solution that integrates with the Exchange server and allows users to independently release new mobile devices from Exchange quarantine after completing two-factor authentication.

The service is implemented as an additional tab in the Axidian Access User Console, where users can manually release their devices from quarantine.

The mobile device provisioning service requires two-factor authentication via the Axidian Access Identity Provider module. If a user has already authenticated in the User Console, they are automatically authenticated in the device provisioning service as well.

Axidian Access API

The Axidian Access API is a REST API interface designed for integration with third-party systems and applications. The API can be used for two main purposes:

1. **Implementing Two-Factor Authentication:**
   If a target application does not support any standard authentication protocols, two-factor authentication can be added by embedding calls to the Axidian Access API. This approach is particularly suitable for custom-built or in-house applications where modifications are feasible.

2. **Integration with Related Systems:**
   Such integration enables additional scenarios for automating credential management or user access control. Examples include integration with:

   - Identity and Access Management (IDM) systems
   - Physical Access Control Systems (ACS)

Integration with Identity Management Systems

Integration with Identity Management (IDM) systems enables the automatic creation and population of user access profiles for the Axidian Access Enterprise SSO module.

A connector to the IDM system allows for automatic synchronization of user credentials in the Enterprise SSO database. Credentials are generated using IDM connectors to the target systems and are immediately saved in the Axidian Access Enterprise SSO subsystem. This eliminates the need for employees to remember or manually enter passwords.

Key benefits of this integration include:

- Enhanced information security, thanks to fully automated password lifecycle management: passwords are created, changed, and input automatically, without any user or administrator involvement.

- Streamlined access provisioning, minimizing steps required for employees to receive access. For example, once a new user is entered into the source system (such as an HR system) and synchronization occurs, the user gains passwordless access to all the systems they need.

Axidian Access Enterprise SSO and IDM Integration Workflow

Let’s examine the integration workflow using the example of onboarding a new employee and using a USB key for authentication when accessing the desktop. The process can be broken down into five main steps:

1. An HR staff member creates a record for the new employee in the HR system.

2. This employee data is transferred to the IDM database via a connector to the HR system.

3. Based on this event, IDM performs a synchronization operation, creating user accounts in all required applications according to the employee’s position (business role). Specialized IDM connectors are used for this task.

4. Similarly, a connector to Axidian Access Enterprise SSO is used. In the final synchronization step, it creates an access profile for the employee in the Enterprise SSO database, copying the user's credentials into it.

5. At this point, the employee has everything needed to begin work. Upon accessing their workstation, the Axidian Access Enterprise SSO agent provides seamless access to all necessary applications by automatically entering the employee’s credentials into application login forms.

Integration with Physical Access Control Systems (PACS)

Integration with physical access control systems (ACS) enables Axidian Access to take into account the physical location of an employee at the moment of authentication. This makes it possible to implement access scenarios such as:

- Allowing access only when the employee is within the building perimeter, for example, after entering through checkpoint No. 1, No. 2, or No. 3

- Restricting access to a specific room, such as Room No. 5, regardless of the route the employee took to reach it

- Granting access from any workstation within a defined zone, for example, any computer located on the third floor.

Axidian Access technical characteristics

User directories	Active Directory DBMS (SQL)
Target resources	Workstations running Microsoft Windows Microsoft Remote Desktop Server Microsoft Internet Information Services Windows desktop applications Web applications VPN servers Application servers Virtual desktop infrastructure (VDI)
Integration mechanisms for target applications	RADIUS ADFS SAML OpenID Connect OAuth 2.0 Kerberos Enterprise Single Sign-On
Authentication technology	Biometrics: fingerprints, palm vein pattern, and face geometry (2D and 3D) Hardware devices: contactless cards, USB tokens, iButtons, and RFID cards One-time passwords: TOTP/HOTP applications, OTP tokens, one-time password delivery via SMS, Telegram and email Push authentication app
Removable hardware tokens	eToken, ID Prime, and iKey (Thales Group, the former SafeNet and Gemalto)
Third-party security solution integration	Permission and user account management tools: Cube, Microsoft FIM, and IBM Tivoli Identity Manager Public key infrastructure management tools: Axidian CertiFlow Tools for information security event monitoring and correlation: SIEM solutions Access monitoring and control tools: Bastion, Orion

About Axidian

Axidian delivers identity and access management solutions designed to enhance cyber resilience for organizations worldwide. With a strong presence in over 25 countries, Axidian has delivered more than 800 projects in access management (IAM), privileged access management (PAM), public key infrastructure (PKI) management, and identity threat detection and response (ITDR) solutions across various sectors.

Axidian offers:

- **One-stop-shop for corporate identity security solutions**
  Our products cover various security scenarios, eliminating the need to work with multiple vendors, complex integrations, and excessive costs.

- **Global support**
  Thanks to a wide network of local partners in more than 30 countries, we provide fast and efficient support, including the availability of on-site specialists.

If you have any questions about our products or need additional information, please visit axidian.com.

Our contacts

axidian.com

sales-europe@axidian.com

sales-mena@axidian.com

sales-asia@axidian.com

www.linkedin.com/company/axidian

HAFS
Distributeur à valeur ajoutée

VOTRE PARTENAIRE TECHNOLOGIQUE
POUR DES INFRASTRUCTURES IT SÉCURISÉES ET PERFORMANTES

EXPERTISE
Des solutions adaptées à chaque environnement

CONFIANCE
Un partenaire fiable à vos côtés

PERFORMANCE
Des infrastructures sécurisées et évolutives

SUPPORT
Un accompagnement technique de qualité

HAFS
Distributeur à valeur ajoutée

Des solutions IT innovantes pour un monde connecté et sécurisé

WIRELESS RADIO
Connectivité sans fil haute performance

RÉSEAUX & SÉCURITÉ IT
Des réseaux fiables et sécurisés

VIRTUALISATION CLOUD
Des solutions Cloud flexibles et évolutives

CYBERSECURITY
Protéger vos données et vos systèmes

VIDÉO PROTECTION
Solutions de vidéosurveillance intelligentes

HCI STOCKAGE SAUVEGARDE
Stockage, sauvegarde et haute disponibilité

SOLUTIONS IT | CYBERSÉCURITÉ | CLOUD | INFRASTRUCTURE RÉSEAU | STOCKAGE | PROTECTION

Département Commercial

HAFS
Distributeur à valeur ajoutée

Vous accompagne

HAFS NETWORKS WCA
+225 07 89 82 56 49 / +225 07 59 05 85 82
sales-ci@hafs-networks.com

HAFS NETWORKS FRANCE
+33 (0)7 49 92 62 57 / +33(0)9 73 89 20 39
sales@hafs-networks.com

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision