IOARX BUSINESS 1.0

IOArx Business Deployment Guide

Install IOArx Central Monitoring, set up your organization, and roll out IOArx Business and IOArx for Browsers to every staff computer.

Document version	1.0
Product	IOArx Business 1.0.0: IOArx Central Monitoring, IOArx Business and IOArx for Browsers (Business)
Date	November 27, 2026
Audience	IT administrators and security engineers

Copyright © 2026 IOArx. All rights reserved.

IOArx Business Deployment Guide
Version 1.0, November 27, 2026

For IOArx Business 1.0.0: IOArx Central Monitoring 1.0.0, IOArx Business 1.0.0 for Windows and Linux, and IOArx for Browsers (Business).

Copyright © 2026 IOArx. All rights reserved.

IOArx, IOArx Business, IOArx Central Monitoring and IOArx for Browsers are products of IOArx. Microsoft, Windows, Windows Server, Microsoft Intune, Microsoft Edge, Google Chrome, Mozilla Firefox and the other names of products and companies in this guide belong to their owners.

The organization, people, computers, accounts and addresses in the examples and screenshots of this guide are fictional.

https://ioarx.com

Contents

1 About This Guide **8**

1.1 Who This Guide Is For . . . 8

1.2 What the Guide Covers . . . 8

1.3 Conventions . . . 9

1.4 The Example Organization . . . 10

1.5 Versions and Release Files . . . 10

1.6 Deployment at a Glance . . . 11

2 How IOArx Business Works **12**

2.1 The Three Parts . . . 12

2.2 Architecture . . . 12

2.3 On Each Computer . . . 13

2.4 How Computers and Central Trust Each Other . . . 14

2.5 What Travels Between Them . . . 15

2.6 What IOArx Business Collects . . . 16

3 Planning the Deployment **18**

3.1 The Central Computer . . . 18

3.2 Staff Computers . . . 18

3.3 Browsers . . . 19

3.4 Network and Firewall . . . 20

3.5 The Address of Central . . . 21

3.6 Licensing, Seats and the Trial . . . 21

3.7 Administrators and Roles . . . 21

3.8 Groups and Access Profiles . . . 22

3.9 Privacy Decisions . . . 22

3.10 A Staged Rollout . . . 23

4 Installing IOArx Central Monitoring 24

4.1 Before You Begin 24
4.2 Run the Installer 24
4.3 What the Installer Sets Up 25
4.4 Check the Service 26
4.5 The Data Folder 26
4.6 The Certificate and Its Fingerprint 27
4.7 The Settings File central.json 27
4.8 Back Up the Keys 28

5 Connecting the Console and First-Time Setup 29

5.1 Open the Console on the Central Computer 29
5.2 Create the Organization and Its Owner 29
5.3 Turn On Two-Factor Sign-In 29
5.4 Require Two-Factor Sign-In 30
5.5 Organization and Support Contact 30
5.6 The Addresses of Central 31
5.7 Use the Console from Another Computer 31
5.8 Sessions, Locking and Shortcuts 32
5.9 The Console at a Glance 32

6 Activating the License 34

6.1 The Trial 34
6.2 Activate a License Key 34
6.3 A Proxy for ioarx.com 35
6.4 License States 35
6.5 Seats 35
6.6 When the License Cannot Be Confirmed 36
6.7 Move the License to Another Central 36

7 Access Profiles 37

7.1 The Four Profiles That Come Ready 37
7.2 Create and Edit a Profile 37
7.3 Files and Folders 39
7.4 Files That Hold Secrets 39

7.5 Network Rules for AI Agents 40
7.6 Programs 41
7.7 AI Agents of Your Organization 41
7.8 Detection 43
7.9 Prompts 43
7.10 Locks 43
7.11 Browser 44
7.12 Privacy 45
7.13 Computers 45
7.14 Limits of a Profile 46
7.15 Simulate 46

8 Groups, People, Administrators and Roles 47
8.1 Groups 47
8.2 Profiles for a Person or a Computer 47
8.3 People 48
8.4 Administrators 48
8.5 Roles 49

9 Deploying IOArx Business 51
9.1 Before You Deploy 51
9.2 Enrollment Tokens 51
9.3 Get the Installers 52
9.4 How Enrollment Works 53
9.5 Install on One Windows Computer 53
9.6 Silent Installation on Windows 54
9.7 What the Installer Does on Windows 55
9.8 Microsoft Intune 56
9.9 Group Policy 57
9.10 Configuration Manager and Other Tools 57
9.11 Install Now, Enroll Later 57
9.12 Linux 58
9.13 Check Enrollment in the Console 60
9.14 Check Enrollment on the Computer 61
9.15 What Staff See 62

10 Deploying IOArx for Browsers **65**

10.1 How the Extension Is Managed 65

10.2 Enter the Store Ids 65

10.3 What IOArx Business Writes on Windows 66

10.4 What IOArx Business Writes on Linux 66

10.5 Firefox 67

10.6 Private Windows 68

10.7 Check the Coverage 68

11 Daily Operations **69**

11.1 The Overview 69

11.2 Approvals of Paused AI Agents 69

11.3 Requests for Access 71

11.4 Incidents 71

11.5 Investigation 73

11.6 Responding on a Computer 74

11.7 Receipts of the Activity Log 75

11.8 Reports and Exports 75

11.9 Forwarding to a SIEM 75

11.10 Updates 78

11.11 Backups and Restore 81

12 Security Model **83**

12.1 Protection on the Staff Computers 83

12.2 Tamper Protection 83

12.3 Signs of Tampering 84

12.4 Uninstall Codes 85

12.5 Limits on Connections and Requests 85

12.6 Administrators of Central 86

12.7 Central Itself 86

12.8 Updates 87

13 Retiring Computers and Uninstalling **88**

13.1 Retire a Computer 88

13.2 Uninstall IOArx Business on a Computer 88

13.3 Install IOArx Business Again . . . 90
13.4 Move Central to Another Computer . . . 90
13.5 Uninstall IOArx Central Monitoring . . . 91

14 Troubleshooting 92
14.1 Where to Look First . . . 92
14.2 Central . . . 92
14.3 Enrollment . . . 93
14.4 Computers Offline . . . 94
14.5 Incomplete Protection . . . 94
14.6 Clocks . . . 95
14.7 Signing In to the Console . . . 95

A Command Reference 97
A.1 IOArx Central Monitoring . . . 97
A.2 On Windows Staff Computers . . . 98
A.3 On Linux Staff Computers . . . 98

B Ports and Addresses 100

C File Locations 101

D Roles and Permissions 103

E Glossary 105

CHAPTER 1

About This Guide

IOArx Business protects the computers of an organization from the risks of AI agents and manages that protection from one place. This guide takes an IT or security team from an empty server to an organization in which every staff computer runs IOArx Business, follows the policy of the organization and reports to IOArx Central Monitoring. It covers planning, installation, configuration, the rollout with Microsoft Intune, Group Policy, Configuration Manager and the package tools of Linux, daily operations, the security model and troubleshooting.

1.1 Who This Guide Is For

This guide is for the IT administrators and security engineers who install IOArx Central Monitoring, deploy IOArx Business to the computers of their organization and run it day to day. It assumes experience with the administration of Windows, with a software distribution tool such as Microsoft Intune, Group Policy or Configuration Manager and, for Linux computers, with the package manager of the distribution.

1.2 What the Guide Covers

Table 1.1: The chapters of this guide

Chapter	What it covers
Chapter 2, How IOArx Business Works	The three parts, how they trust each other, what travels between them and what IOArx Business collects.
Chapter 3, Planning the Deployment	Requirements, network and firewall, the address of Central, licensing, administrators, groups, profiles and privacy.
Chapter 4, Installing IOArx Central Monitoring	The installer, the service, the data folder, the certificate and the first backup of the keys.
Chapter 5, Connecting the Console and First-Time Setup	The organization, the Owner, two-factor sign-in and consoles on other computers.
Chapter 6, Activating the License	The trial, activation, seats, and how Central keeps the license confirmed.
Chapter 7, Access Profiles	Every part of a profile: rules for files and folders, secrets, network, programs, AI agents, detection, prompts, locks, browser, privacy and computers.
Chapter 8, Groups, People, Administrators and Roles	Which profile each computer follows and what each administrator may do.
Chapter 9, Deploying IOArx Business	Enrollment tokens and the installation on Windows and Linux: interactive, silent, and with management tools.

Chapter	What it covers
Chapter 10, Deploying IOArx for Browsers	The managed extension in Chrome, Edge and Firefox.
Chapter 11, Daily Operations	Approvals, requests for access, incidents, investigation, response on computers, reports, SIEM forwarding, updates and backups.
Chapter 12, Security Model	How IOArx Business protects itself and the data it handles.
Chapter 13, Retiring Computers and Uninstalling	Retirement, uninstall codes, a second installation on the same computer, and the removal of Central.
Chapter 14, Troubleshooting	Enrollment, offline computers, incomplete protection, network, clocks, logs and sign-in.
Appendices	Command reference, ports and addresses, file locations, roles and permissions, and a glossary.

1.3 Conventions

Table 1.2: Conventions of this guide

Example	Meaning
Approvals	The name of a page, tab, field or button of an app, as it appears on the screen.
Settings › **Server**	A page of the console of IOArx Central Monitoring, then a tab or a part of that page.
`sc query IOArxCentral`	A command, file name, folder, registry key or value that you type exactly as shown.
`<enrollment token>`	A value to replace with your own, without the angle brackets.

Commands appear in boxes whose title says where to run them. Type each command on one line. In the rare case that a line is too long for the page, an arrow marks where it continues:

Command Prompt or PowerShell, as an administrator

```
sc query IOArxCentral
```

Three kinds of boxes stand out from the text:

> **Note.** Background or a detail that helps with the task at hand.

> **Important.** A setting or a step that later steps depend on.

> **Warning.** An action that cannot be undone, or that changes every computer of the organization.

1.4 The Example Organization

The examples and the screenshots of this guide use Northbridge Analytics, a fictional organization. Replace its names and addresses with those of your organization.

Table 1.3: Names and addresses of the example organization

Item	In the examples
Organization	Northbridge Analytics
DNS domain	`northbridge.example`
Windows domain	`NORTHBRIDGE`, with accounts such as `NORTHBRIDGE\mmorgan`
Central computer	`central.northbridge.example`, IP address `10.20.0.15`
First administrator (Owner)	Dana Whitfield, user name `dana.whitfield`
File share for installers	`\\fs01.northbridge.example\deploy\ioarx`
SIEM	`siem.northbridge.example`

1.5 Versions and Release Files

This guide describes IOArx Business 1.0.0. IOArx publishes its release files at `https://ioarx.com/updates/business/`.

Table 1.4: Release files of IOArx Business 1.0.0

File	What it installs
`IOArx-Central-Monitoring_1.0.0_x64-setup.exe`	IOArx Central Monitoring for 64-bit Windows: the IOArx Central service and the console on the Central computer, or the console alone on the computers of administrators.
`IOArx-Business_1.0.0_x64-setup.exe`	IOArx Business for 64-bit Windows.
`IOArx-Business_1.0.0_x86-setup.exe`	IOArx Business for 32-bit Windows.
`ioarx-business_1.0.0_amd64.deb`	IOArx Business for Ubuntu 22.04 or later, Debian 12 or later and the distributions built on them.
`ioarx-business-1.0.0-1.x86_64.rpm`	IOArx Business for Fedora and openSUSE Tumbleweed.

Every Windows program and installer of IOArx Business carries a code signature with a time stamp. Every package of IOArx Business is also signed with the update key of IOArx, which Central and every computer check before they install an update (Section 11.10). This signature is published next to each file, in a file of the same name with `.sig` added, such as `IOArx-Business_1.0.0_x64-setup.exe.sig`. Once IOArx Central Monitoring runs, it downloads the packages of IOArx Business itself and offers them on its **Deployment** page (Section 9.3).

1.6 Deployment at a Glance

A complete deployment follows these steps. Each step points to the part of the guide that describes it.

1. Plan the deployment: choose the Central computer and give it a DNS name, open TCP port 9743 from the staff computers to Central, let Central reach `ioarx.com`, and decide on groups, profiles, administrators and privacy (Chapter 3).
2. Install IOArx Central Monitoring on the Central computer and copy its keys to a safe place (Chapter 4).
3. On the Central computer, create the organization and its Owner, and turn on two-factor sign-in (Chapter 5).
4. Activate the license, or start with the trial of 14 days for up to 10 computers (Chapter 6).
5. Check the addresses of Central under **Settings** › **Server** before you create the first enrollment token (Section 5.6).
6. Prepare access profiles and groups, and add the other administrators (Chapters 7 and 8).
7. Enter the store ids of IOArx for Browsers (Business) (Chapter 10).
8. Create an enrollment token and install IOArx Business on a pilot group of computers (Chapter 9).
9. Review the pilot in the console, adjust the profiles, then roll IOArx Business out to every computer (Chapters 9 and 11).
10. Set up forwarding to your SIEM, backups of Central, and the rollout of updates (Chapter 11).

CHAPTER 2

How IOArx Business Works

IOArx Business watches the AI agents on the computers of an organization: the files they open, change, rename and delete, the hosts they connect to and the programs they start. Rules in an access profile decide what each AI agent may do. A rule allows an access, blocks it, or asks: the AI agent then waits, paused with every process it started, until an administrator or the person at the computer answers. IOArx Central Monitoring keeps the profiles, the records and the decisions of the whole organization in one place.

IOArx Business recognizes AI agents with a built-in catalog: by the signature of a program, its app package, its file, its folder, its command line or its environment. Behavior detection finds AI agents that no catalog names. An organization adds its own AI agents to the catalog in its access profiles.

2.1 The Three Parts

Table 2.1: The parts of IOArx Business

Part	Where it runs	What it does
IOArx Central Monitoring	The IOArx Central service on one Windows computer or server of the organization, the Central computer; the console there and on the computers of administrators	The IOArx Central service keeps the database of the organization and talks to every staff computer. The console is the app in which administrators sign in, watch, investigate, respond, and set the policy.
IOArx Business	Every staff computer: Windows, 64-bit and 32-bit, and Linux	A service enforces the access profile that Central sends, from the start of the computer, and reports to Central. The app shows each person the state of protection, their own activity, the alerts that wait and their requests to administrators.
IOArx for Browsers (Business)	Chrome, Edge and Firefox on staff computers	Installed by browser policy, it checks prompts, pastes and uploads on AI services, and reports what it stops to IOArx Business on the same computer.

2.2 Architecture

Figure 2.1 shows the parts and the connections between them. Every staff computer and every console reaches Central on one TCP port, 9743, over HTTPS. Central reaches `ioarx.com` over HTTPS to confirm its license and to download updates, and it forwards events to the SIEM of the

organization when forwarding is on. Staff computers never connect to `ioarx.com`: they receive their policy, their commands and their updates from Central.

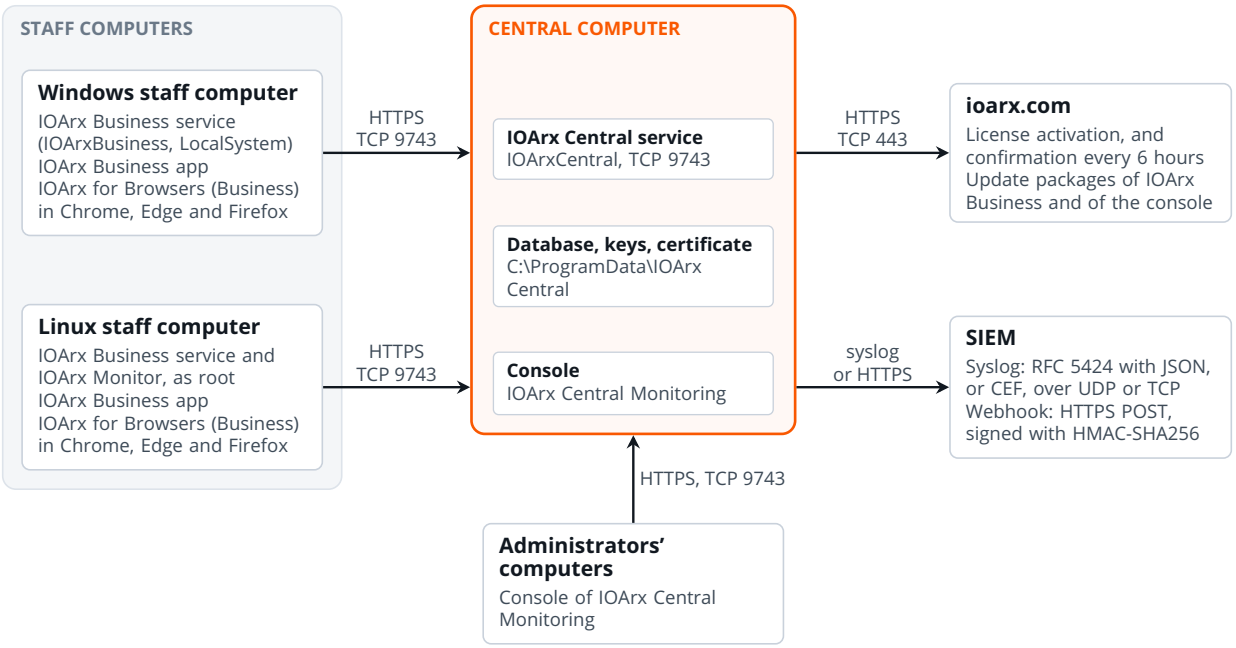


Figure 2.1: The parts of IOArx Business and their connections

Everything that Central collects stays in its database, on the organization's own computer. IOArx receives none of it (Section 2.6).

2.3 On Each Computer

2.3.1 Windows staff computers

Three programs of IOArx Business run on a Windows staff computer:

- `ioarx-endpoint.exe` runs as the Windows service `IOArxBusiness`, with the display name IOArx Business, as LocalSystem. It starts with Windows, before anyone signs in, and Windows starts it again after a failure. It watches file activity through a trace session of Event Tracing for Windows of its own, `IOArx Business File Monitor`, enforces the access profile, pauses and stops AI agents, applies folder locks and browser policies, and talks to Central.
- `IOArx Business.exe`, the app, starts at every sign-in through the registry key `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`, in the background, with its icon in the notification area. It runs with the rights of the person signed in and talks to the service over the named pipe `\\.\pipe\IOArxBusiness`. When it does not run in the session of a signed-in person, the service starts it there again, unless the profile lets staff close it.
- Browsers start `ioarx-endpoint.exe` as their native messaging host when IOArx for Browsers (Business) connects. It relays between the extension and the service.

The service keeps its data in `C:\ProgramData\IOArx Business`, which only SYSTEM and the administrators of the computer can open.

2.3.2 Linux staff computers

- `ioarx-monitor`, IOArx Monitor, runs as the systemd service `ioarx-monitor.service`, as root. It watches file activity with fanotify, processes with the process connector of the kernel, connections with nftables and the netfilter queue 4242, and name lookups with the netfilter queue 4243.
- `ioarx-endpoint` runs as the systemd service `ioarx-business.service`, as root. It runs the protection engine, connects to IOArx Monitor as its system client, and talks to Central.
- The app, `ioarx-business`, starts at every sign-in to a desktop session through `/etc/xdg/autostart/ioarx-business.desktop`. It talks to the service over the socket `/run/ioarx-business.sock`, which tells the service the user id of each connection.

The service keeps its data in `/var/lib/ioarx-business`, which only root can open.

2.3.3 The Central computer

- `ioarx-central-server.exe` runs as the Windows service `IOArxCentral`, with the display name IOArx Central Monitoring, under its own virtual account `NT SERVICE\IOArxCentral`, not as LocalSystem. It starts with Windows and listens on TCP port 9743 on every address of the computer. It keeps the database of the organization in `C:\ProgramData\IOArx Central`, which only SYSTEM, the administrators of the computer and the service account can open.
- `IOArx Central Monitoring.exe`, the console, connects to the service over HTTPS: at `127.0.0.1:9743` on the Central computer, or at the address of Central from another computer. Every request of the console carries the session token of the administrator who signed in.

2.4 How Computers and Central Trust Each Other

One port, HTTPS only

Computers and consoles reach Central over HTTPS with TLS 1.2 or 1.3, on one TCP port, 9743. Computers call the agent API under `/api/agent/v1/`; the console calls the admin API under `/api/admin/v1/`.

A pinned certificate

At its first start, Central makes an ECDSA P-256 key and a self-signed certificate that is valid for 25 years. Computers and consoles ask no certificate authority about it. They compare the SHA-256 hash of the certificate with the pin they hold and refuse any other certificate during the TLS handshake, before any data is sent, even one that a public authority signed. Computers receive the pin inside their enrollment token. A console learns it at its first connection, after an administrator has compared the fingerprint of the certificate (Section 5.7).

A key for each computer

At enrollment, each computer makes an Ed25519 key pair and gives Central only the public key. It signs every later request. The signature covers the method, the path, the time, a random nonce and the SHA-256 hash of the body. Central accepts a time within five minutes of its own clock and each nonce once, so a recorded request cannot be sent again. The database of Central holds no secret with which anyone could speak for a computer.

Enrollment tokens

An enrollment token is one line of text that starts with `IOXB1.`. It carries the addresses of Central, its port, the pin of its certificate, the name of the organization and a secret of 128 bits. Central keeps only the SHA-256 hash of the secret, together with the expiry of the token, the number of computers that may use it and the group that new computers join. After enrollment, every new policy brings the computer the current addresses of Central.

Administrators

Administrators sign in to the console with a user name and a password, and with a code of an authenticator app when two-factor sign-in is on. Chapter 12 describes passwords, sessions, lockouts, roles and scopes.

2.5 What Travels Between Them

Table 2.2: What travels between a staff computer and Central

Exchange	When	What it carries
Enrollment	Once, when IOArx Business is installed with a token	From the computer: the secret of the token, the public key of the computer, its name, system and version, its domain, the accounts signed in, and a hash of the identifier of the machine. From Central: the id of the computer, its first policy, the secret behind its uninstall code, and the standing of its license seat.
Heartbeat	Every 30 seconds, as set under **Settings** › **Computers**	From the computer: its version, the state of protection, the version of its policy, the head of its activity log, the accounts signed in, its browsers and its locks. From Central: the standing of the seat, a new policy when there is one, waiting commands, and the offer of an update.
Commands	At once	The computer keeps one request open, which Central answers as soon as a command waits: the answer to an approval request, stopping an AI agent, a message, a receipt of the activity log, a restart of the service, or retirement.
Activity	Continuously, in batches	Every record of the activity log with its hash and the hash before it, the events of IOArx for Browsers, behavior detections, the use of AI services, and the events of the service itself.
Approval requests	When a rule says Ask and an administrator answers	The AI agent, the file or host, the person, the programs behind the request, what the file holds, and the deadline.
Inventory	Every 10 minutes, and whenever it changes	The AI agents that run on the computer.
Updates	When the rollout offers a newer version	The package of IOArx Business, which the computer downloads from Central.

Changes of the policy, folder locks and isolation reach a computer with its next heartbeat. A computer that cannot reach Central keeps enforcing the last policy it received. Its activity log keeps

every record until Central has it, and up to 20,000 other events wait in a queue of their own. The computer sends them as soon as Central answers again.

2.6 What IOArx Business Collects

IOArx Business protects the data of an organization from AI agents; it does not watch the people of the organization. Staff read the same facts, and the privacy notice of the organization, in the IOArx Business app under **Privacy**.

What is collected

On each staff computer, about AI agents, AI apps and the programs they start:

- the files they open, change, rename and delete, with the decision of the rules and what decided it;
- the hosts they connect to, with the decision;
- the programs behind each access: program files, publishers, and command lines with every secret that the detectors find replaced by its kind, or less, as the profile sets;
- what behavior detection found: the program, the confidence and the signals behind it;
- the AI agents that run on the computer.

From the browsers, with IOArx for Browsers (Business):

- what it stopped on the AI services it protects: the service, the action, the kind and number of findings, and the names of flagged files with the reason;
- which AI services the browsers reach, counted per hour from their name lookups.

About the computer: its name, its system and version, the accounts signed in, and the state of protection.

What is never collected

- The contents of files. IOArx Business reads files on the computer to find secrets; only the kind and number of what it found leave the computer.
- The text of prompts, or the secrets found in them.
- Browsing outside the AI services that IOArx for Browsers protects.
- What people type or do in programs that are not AI agents.
- Screens, keystrokes, cameras or microphones.

2.6.1 Where the data lives

Everything that Central collects stays in the database of IOArx Central Monitoring, on the organization's own computer. IOArx receives none of it. Central talks to `ioarx.com` only to confirm its license and to download updates. Its license requests carry the license key when Central activates it, and afterwards the activation that `ioarx.com` gave in its place; the name of the product; an identifier of the Central installation, made as a hash of the identifier of the Central computer so that the identifier itself never leaves it; the name of the Central computer, so that the owner of a license can tell installations apart; and the version of Central. The downloads of updates carry nothing about the organization.

2.6.2 Controls of the organization

Table 2.3: Privacy controls and where to set them

Control	Where	What it does
Command lines	Each access profile, **Privacy**	With secrets taken out (the default), only the program, or not at all.
File paths	Each access profile, **Privacy**	Full paths (the default), or only the folder.
Privacy notice	Each access profile, **Privacy**	The notice that staff read in the app. Empty: the built-in notice.
Own activity	Each access profile, **Computers**	Whether staff see in the app what is reported about them.
Pseudonyms	**Settings** › **Retention and privacy**	People appear as pseudonyms, such as Person 7F3A, to administrators without the permission to see the names behind them. Each look behind a pseudonym goes into the audit log.
Retention	**Settings** › **Retention and privacy**	Central deletes events older than the retention period: 180 days by default, 30 to 3,650 days.
Roles and scopes	**Roles** and **Administrators**	Administrators see only what their role allows, and only the groups of their scope.

CHAPTER 3

Planning the Deployment

A few decisions made before the installation save work later: which computer runs Central and under which name the staff computers reach it, what the network lets through, how many seats the organization needs, who administers IOArx Business, which computers follow which access profile, and what the organization collects. This chapter goes through them in that order.

3.1 The Central Computer

Table 3.1: Requirements of the Central computer

Item	Requirement
Operating system	Windows 10 or Windows 11, or Windows Server 2019 or later, 64-bit.
Memory	4 GB for a few hundred computers.
Disk	20 GB of free space for a few hundred computers, on the drive that holds `C:\ProgramData`.
Availability	Always on. Staff computers report to Central, and AI agents that wait for an administrator wait for Central.
Network	Reachable by every staff computer and every console on TCP port 9743, and able to reach `ioarx.com` over HTTPS (Section 3.4).
Name	A DNS name that every staff computer resolves (Section 3.5).
Components	Microsoft Edge WebView2 Runtime, for the console. Windows 11 includes it; where it is missing, the installer installs it from Microsoft.
Rights	An administrator of the computer runs the installer.
Clock	Synchronized with the time source of the organization (Section 14.6).

Choose a computer that only the security team administers. An administrator of the Central computer can open the data folder of Central, stop its service, and give an Owner a new password with the command `reset-owner` (Section 11.11.2).

On the computers of administrators, the console alone needs 64-bit Windows, Microsoft Edge WebView2 Runtime, and a network path to Central on TCP port 9743. It runs no service there and opens no port (Section 5.7).

3.2 Staff Computers

IOArx Business runs on Windows and Linux staff computers that meet the requirements of Tables 3.2 and 3.3.

Table 3.2: Requirements of Windows staff computers

Item	Requirement
Operating system	Windows 11 or Windows 10, 64-bit, with `IOArx-Business_1.0.0_x64-setup.exe`; Windows 10, 32-bit, with `IOArx-Business_1.0.0_x86-setup.exe`.
Components	Microsoft Edge WebView2 Runtime, for the app. Windows 11 includes it; where it is missing, the installer installs it from Microsoft and stops if it cannot.
Rights	An administrator of the computer, or SYSTEM through a management tool, runs the installer.
Network	TCP port 9743 to Central.
Other software	IOArx Personal is uninstalled before IOArx Business is installed.

Table 3.3: Requirements of Linux staff computers

Item	Requirement
Processor	64-bit x86 (`x86_64`).
Distribution	With systemd. The deb package for Ubuntu 22.04 or later, Debian 12 or later and the distributions built on them; the rpm package for Fedora and openSUSE Tumbleweed.
Libraries	glibc 2.34 or later, WebKitGTK 4.1 and GTK 3, OpenSSL 3, nftables and the AppIndicator library. The package manager installs them together with the package.
Kernel	fanotify and the netfilter queue, as the kernels of these distributions provide. Linux 5.9 or later also reports deletions and renames of files.
Rights	root, through `sudo`.
Network	TCP port 9743 to Central.
Other software	The package of IOArx Business replaces the package of IOArx Personal, `ioarx`, when it is installed.

IOArx Business takes the place of IOArx Personal. On Windows, uninstall IOArx Personal before you install IOArx Business: Central reports a computer that still has it as a sign of tampering, **IOArx Personal is installed on this computer as well** (Table 12.1). On Linux, the package of IOArx Business replaces IOArx Personal: apt removes it by itself, dnf needs the option `--allowerasing`, and zypper asks, or takes `--force-resolution` when it runs without questions (Section 9.12).

3.3 Browsers

Table 3.4: Browsers that IOArx for Browsers (Business) supports

Browser	How IOArx Business installs the extension
Google Chrome 120 or later	From the Chrome Web Store, by browser policy, with the store id you enter under **Settings** › **Browser extension**.
Microsoft Edge 120 or later	From Microsoft Edge Add-ons, by browser policy, with the store id you enter under **Settings** › **Browser extension**.

Browser	How IOArx Business installs the extension
Mozilla Firefox 140 or later	From the package signed by Mozilla, `ioarx-business.xpi`, when the install folder of IOArx Business holds it, by browser policy (Section 10.5).

3.4 Network and Firewall

Table 3.5: Connections of IOArx Business

From	To	Port	Purpose
Staff computers	Central	TCP 9743, HTTPS	Enrollment, heartbeats, commands, activity, approval requests, update packages.
Administrators' computers	Central	TCP 9743, HTTPS	The console.
Central	`ioarx.com`	TCP 443, HTTPS	License activation and confirmation, the update feed, the packages of IOArx Business and the newest installer of IOArx Central Monitoring.
Computers with the console	`ioarx.com`	TCP 443, HTTPS	New versions of IOArx Central Monitoring, when an administrator checks for them.
Central	Syslog server	UDP or TCP, 514 by default	Forwarding of events to syslog, when it is on.
Central	Webhook	HTTPS, the address you enter	Forwarding of events to a webhook, when it is on.
Browsers of staff computers	Chrome Web Store, Microsoft Edge Add-ons	TCP 443, HTTPS	Installation and updates of IOArx for Browsers (Business).
Staff computers	Microsoft	TCP 443, HTTPS	Only during installation, and only where Microsoft Edge WebView2 Runtime is missing.

The installer of IOArx Central Monitoring adds the inbound rule `IOArx Central Monitoring` to Windows Firewall on the Central computer: TCP port 9743, for the program `ioarx-central-server.exe`, in every network profile. Open the same port on every firewall between the staff computers and Central.

Staff computers and consoles connect to Central directly. They use no proxy. Central reaches `ioarx.com` directly, through the proxy settings of the system, or through a proxy that you enter under **Settings** › **Network** (Section 6.3).

3.4.1 Offices behind one address

Every staff computer keeps one connection to Central open. Central holds at most 1,000 connections from one network address, which is one IPv4 address or one IPv6 `/64` network, and 20,000 connections in all. When more than 1,000 staff computers reach Central through one address, for

example from an office behind one NAT, raise the limit per address in `central.json` (Section 4.7).

3.5 The Address of Central

Staff computers find Central by the addresses listed under **Settings** › **Server**, in the order given there. Every new enrollment token carries the list, and every new policy brings enrolled computers the current list. Until you set the addresses, Central lists the name of the Central computer and each of its IP addresses.

Give Central a DNS name that stays the same, such as `central.northbridge.example`, and list it first under **Settings** › **Server**. Computers trust Central by its certificate, not by its name or address. Each computer tries the addresses of its newest policy first, then the ones it knew before, up to 12 in all. If Central moves to another computer with the same name, change the DNS record: computers reach the new computer as long as it keeps the certificate of Central (Section 13.4).

> **Important.** To give Central a new name or address, add it under **Settings** › **Server** while the old one still works. Wait until the computers in use have called in and applied their newest policy: the chip **Policy not applied** under **Computers** shows how many have not. Then remove the old address. A computer that was offline during the change receives the new address at its next call through an address it still knows.

3.6 Licensing, Seats and the Trial

The license of IOArx Business covers a number of computers, its seats. Plan the seats for every Windows and Linux computer that will run IOArx Business.

- Each enrolled computer takes one seat, and retiring a computer frees its seat. Central refuses enrollments when every seat is taken. Staff never see a license screen.
- Without a license key, Central runs a trial of 14 days for up to 10 computers, counted from its first start.
- Central confirms its license with `ioarx.com` every 6 hours and keeps working for 14 days without reaching it.
- A staff computer protects while Central has confirmed its seat within the last 30 days. Set this period, from 1 to 90 days, under **Settings** › **Computers**.
- A computer that joins again with a new token, after Central retired it, after its uninstall code was given, or after its system was installed again, becomes a new record with a seat of its own. Retire its earlier record if that one is still active (Section 13.3).

Chapter 6 describes activation, the states of a license, and what happens when Central or a computer cannot confirm it.

3.7 Administrators and Roles

Every administrator has one role and a scope: the whole organization, or some groups of computers with their people and events. Central comes with six roles. Organizations add roles of their own (Section 8.5).

Table 3.6: The built-in roles

Role	What it allows
Owner	Everything, including the license and the other Owners.
Administrator	Everything except the license. Cannot change Owners.
Security Analyst	Investigates events, works on incidents, answers approval requests, and responds on computers.
Helpdesk	Enrolls computers, answers approval requests, and looks after computers and people.
Auditor	Reads everything, including the audit log, and changes nothing.
Privacy Officer	Reviews what is collected and who looked at it, and sees the names behind pseudonyms.

When you plan the administrators:

- Name at least two Owners. Only an Owner gives or takes the Owner role, and the last Owner keeps it.
- Give each administrator the narrowest role that covers their work, and limit the scope of administrators who look after one region or department to its groups.
- Decide who answers approval requests. AI agents wait for an answer, so the people who answer need to be reachable during working hours. The roles Owner, Administrator, Security Analyst and Helpdesk answer approval requests.
- Plan two-factor sign-in for every administrator. Central can require it (Section 5.4).

3.8 Groups and Access Profiles

Each computer follows one access profile. Central decides which one in the order of Figure 3.1: the profile set on the computer itself, else the own profile of its person, else the profile of its group or of the nearest group above it, else the default profile of the organization.

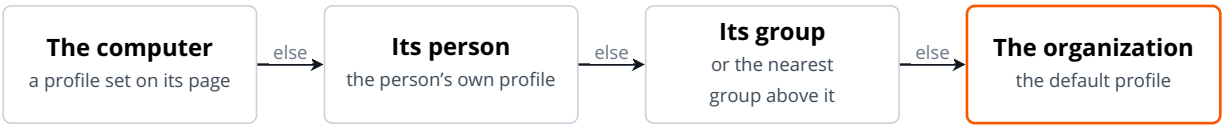


Figure 3.1: How Central chooses the access profile of a computer

Plan groups by the profile their computers need, for example by department, by location or by kind of computer. A computer joins the group of the enrollment token it uses, so plan one token for each group (Section 9.2). Four profiles come ready: **Standard**, the default, **Locked down**, **Developers** and **Monitor only** (Section 7.1).

3.9 Privacy Decisions

Agree on the following settings with the people responsible for privacy in your organization before the rollout, and write the notice that staff read in the app.

Table 3.7: Privacy decisions and their defaults

Decision	Where	Default
How much of command lines leaves the computers	Access profile, **Privacy**	With secrets taken out
How much of file paths leaves the computers	Access profile, **Privacy**	Full paths
The notice that staff read	Access profile, **Privacy**	The built-in notice
Whether staff see their own activity	Access profile, **Computers**	On
Whether people appear by pseudonym	**Settings** › **Retention and privacy**	Off
Whether accounts make new people	**Settings** › **Retention and privacy**	On
How long Central keeps events	**Settings** › **Retention and privacy**	180 days
Who sees the names behind pseudonyms	**Roles**	Owner, Administrator, Privacy Officer

3.10 A Staged Rollout

Roll IOArx Business out in stages:

1. Start with a pilot group of a few computers of the IT and security teams. Give the group a profile made from **Monitor only**: it records and reports what AI agents do and stops nothing, so the pilot shows which AI agents run and which files and hosts they use.
2. Switch the pilot group to the profile you plan for the organization, such as **Standard**. Answer the approval requests for some days and keep frequent answers as rules (Section 11.2).
3. Roll out group by group, with one enrollment token for each group, and watch **Computers** and **Approvals** after each step.

CHAPTER 4

Installing IOArx Central Monitoring

One installer, `IOArx-Central-Monitoring_1.0.0_x64-setup.exe`, installs IOArx Central Monitoring in one of two roles: on the Central computer, the IOArx Central service with the console; on the computers of administrators, the console alone (Section 5.7). This chapter sets up the Central computer that you chose in Section 3.1.

4.1 Before You Begin

- The Central computer meets the requirements of Table 3.1, and you are signed in to it as one of its administrators.
- The DNS name of Central exists and points to the Central computer (Section 3.5).
- The firewalls between the staff computers and Central let TCP port 9743 through, and Central reaches `ioarx.com` over HTTPS (Section 3.4).
- You have the installer, from `https://ioarx.com/updates/business/`.
- A safe place for a copy of the keys of Central is ready, such as an encrypted share or a password vault that only the security team opens (Section 4.8).

Check the code signature of the installer before you run it. In PowerShell, in the folder of the installer:

PowerShell

```
Get-AuthenticodeSignature .\IOArx-Central-Monitoring_1.0.0_x64-setup.exe
```

The column `Status` shows `Valid`. Do not run an installer whose signature is not valid.

4.2 Run the Installer

1. On the Central computer, run `IOArx-Central-Monitoring_1.0.0_x64-setup.exe`. Windows asks for the rights of an administrator; allow them.
2. On **Welcome to IOArx Central Monitoring Setup**, choose **Next**.
3. On **License Agreement**, read the license agreement and choose **I Agree**.
4. On **Choose Install Location**, keep `C:\Program Files\IOArx Central Monitoring` and choose **Next**.
5. On **Choose Start Menu Folder**, keep the folder `IOArx`, so that the console appears in the Start menu, and choose **Install**.
6. When the installer asks **Should this computer run IOArx Central Monitoring for your organization?**, choose **Yes**.

7. Wait until the installer has finished, then choose **Finish**.

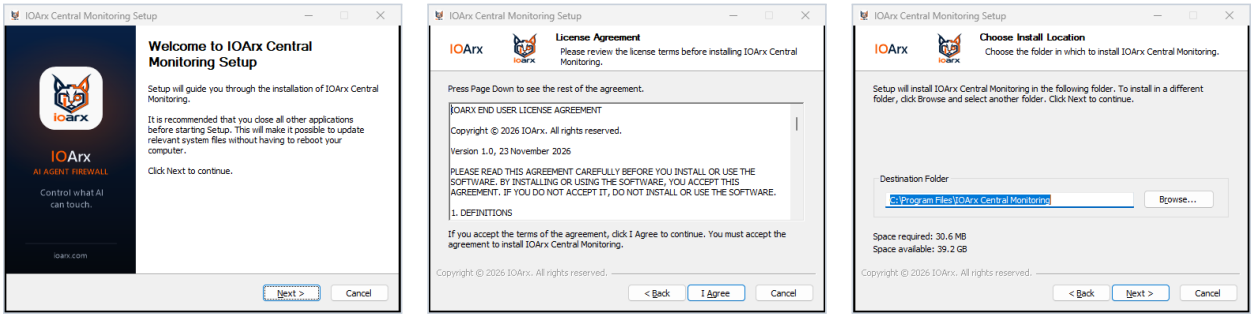


Figure 4.1: The installer of IOArx Central Monitoring: Welcome, License Agreement and Choose Install Location

The installer installs Microsoft Edge WebView2 Runtime where it is missing, copies the programs, then sets up and starts the IOArx Central service. If the service cannot be set up, the installer shows the reason under **The IOArx Central Monitoring service could not be set up** and stops; Section 14.2 lists the usual causes.

To install the Central computer without a window, run the installer with `/S` as an administrator. It installs the IOArx Central service and the console; `/S /CONSOLE` installs the console alone. An update, and the installer run again, keep the role that the computer has (Section 11.10.2).

Command Prompt, as an administrator, on the Central computer

```
IOArx-Central-Monitoring_1.0.0_x64-setup.exe /S
```

4.3 What the Installer Sets Up

Table 4.1: What the installer of IOArx Central Monitoring sets up

Item	Details
Programs	`C:\Program Files\IOArx Central Monitoring`: the console `IOArx Central Monitoring.exe`, the service program `ioarx-central-server.exe`, and `uninstall.exe`.
Service	`IOArxCentral`, display name IOArx Central Monitoring. Automatic start, under the virtual account `NT SERVICE\IOArxCentral`. After a failure, Windows starts it again after 5, 15 and 60 seconds.
Data folder	`C:\ProgramData\IOArx Central`, open to SYSTEM, the administrators of the computer and the service account only, without inherited entries. Its folder `public` is readable by every user of the computer, so that the console finds the Central of its own computer.
Firewall	The inbound rule `IOArx Central Monitoring` of Windows Firewall: the TCP port of `central.json`, 9743, for the program `ioarx-central-server.exe`, in every network profile.
Certificate	Made by the service at its first start: `tls\key.pem` and `tls\cert.pem` in the data folder.
Start menu	The folder `IOArx`, with IOArx Central Monitoring.

On the computer of an administrator, where the answer to the question of the installer is **No** or the installation runs with `/CONSOLE`, the installer sets up the programs and the Start menu folder only: no service, no data folder, no firewall rule and no open port.

4.4 Check the Service

On the Central computer, in a Command Prompt that runs as an administrator, check the service, the firewall rule and the certificate:

Command Prompt, as an administrator, on the Central computer

```
sc query IOArxCentral
netsh advfirewall firewall show rule name="IOArx Central Monitoring"
"C:\Program Files\IOArx Central Monitoring\ioarx-central-server.exe" print-pin
```

`sc query` shows `STATE: 4 RUNNING`. `print-pin` prints the port, the pin and the fingerprint of the certificate.

From a staff computer, check that Central answers on its port. `curl.exe` comes with Windows 10 and Windows 11; Linux distributions call it `curl`:

Command Prompt or PowerShell, on a staff computer

```
curl.exe -k https://central.northbridge.example:9743/api/admin/v1/setup
```

Central answers with a short JSON text that holds its version and whether it waits for its first setup. The option `-k` lets `curl` accept the self-signed certificate for this test; computers and consoles check the certificate by its pin.

4.5 The Data Folder

Table 4.2: The data folder of Central, `C:\ProgramData\IOArx Central`

Path	What it holds
`central.db`	The database of the organization, in WAL mode, with `central.db-wal` and `central.db-shm` beside it.
`central.json`	Settings that the service reads at its start: the port, and optionally the address to listen on and the number of connections per address (Section 4.7).
`tls\key.pem`, `tls\cert.pem`	The key and the self-signed certificate of Central, valid for 25 years. Every computer pins this certificate.
`keys\vault.key`	The key that seals, in the database, the keys of two-factor sign-in, the secrets behind uninstall codes, the webhook secret and the proxy.
`public\server.json`	The version, port, pin, fingerprint and addresses, for the console on the same computer.
`packages\`	Update packages of IOArx Business, each checked against the signature of IOArx.

Path	What it holds
`backups\`	Backups of the database, made with **Make a backup now**. Central keeps the newest 10.
`logs\central.log`	The log of the service. It holds no passwords, tokens, keys or contents of events.

4.6 The Certificate and Its Fingerprint

The service makes its certificate at its first start and keeps it in the folder `tls`. The pin is the SHA-256 hash of the certificate, written as 43 characters of base64url. The fingerprint is the same hash as 16 groups of four hexadecimal digits, for people to compare by eye. Both appear under **Settings** › **Server**, on the **Deployment** page, and in the output of `print-pin`.

Computers and consoles trust exactly this certificate. A Central with another certificate is a stranger to every computer that enrolled before, so the folder `tls` must survive every move and every restore of Central (Section 4.8).

4.7 The Settings File central.json

The service reads `C:\ProgramData\IOArx Central\central.json` at its start. The first installation writes it with the port, `{ "port": 9743 }`. Updates and new installations keep the file as it is, and the installer opens the firewall for the port it names. The file takes three settings:

Table 4.3: Settings of central.json

Setting	Meaning
`port`	The TCP port of Central: 9743.
`bind`	One IP address to listen on, such as `10.20.0.15`. Without it, Central listens on every IPv4 and IPv6 address of the computer.
`connections_per_address`	The most connections that Central holds from one network address, from 16 to 20,000. Without it, 1,000.

To let up to 5,000 staff computers reach Central through one address:

1. Open `central.json` in an editor that runs as an administrator, and write:

   C:\ProgramData\IOArx Central\central.json

   ```
   { "port": 9743, "connections_per_address": 5000 }
   ```

2. Restart the service:

   Command Prompt, as an administrator, on the Central computer

   ```
   sc stop IOArxCentral
   sc start IOArxCentral
   ```

Important. Keep the port 9743. Enrollment tokens and policies carry the port, and a computer reaches Central only on a port it knows.

4.8 Back Up the Keys

Copy the folders `tls` and `keys` of the data folder to a safe place right after the installation. `tls` holds the certificate that every computer pins. `keys` holds the key that seals the secrets in the database. Without `tls`, a restored Central has a new certificate that no computer trusts, and every computer must join it again as a new computer (Section 11.11.1). Without `keys`, two-factor sign-in must be set up again, the webhook secret and the proxy must be entered again, and Central can no longer show the uninstall codes of the computers.

Command Prompt, as an administrator, on the Central computer

```
robocopy "C:\ProgramData\IOArx Central\tls" "<backup folder>\tls" /E
robocopy "C:\ProgramData\IOArx Central\keys" "<backup folder>\keys" /E
```

Warning. Treat the copy like any private key. Whoever holds `tls\key.pem` can present the certificate of Central, and whoever holds `keys\vault.key` together with a copy of the database can open the secrets sealed in it. Keep the copy where only the security team can open it.

Section 11.11 describes the regular backups of the database, which you keep together with this copy.

CHAPTER 5

Connecting the Console and First-Time Setup

The first start of the console sets up the organization and its first administrator, the Owner. Central takes this setup only from the computer it runs on, so nobody on the network can make themselves the Owner of a Central that was just installed. Do the steps of this chapter on the Central computer, then connect consoles on other computers.

5.1 Open the Console on the Central Computer

1. On the Central computer, open **IOArx Central Monitoring** from the Start menu.
2. On **Connect to IOArx Central**, choose **IOArx Central on this computer**. It shows the version of Central and the address `127.0.0.1:9743`, marked **Found**.

A new Central opens its setup, which has three steps.

5.2 Create the Organization and Its Owner

1. On **Name your organization**, type the name of the organization in **Organization**, such as Northbridge Analytics, and choose **Continue**. Staff see this name in IOArx Business, and every enrollment token carries it.
2. On **Create the first administrator**, type **Your name**, a **User name** and an **Email**, and choose **Continue**. A user name has 3 to 64 letters, digits, dots, hyphens or underscores. This administrator becomes the Owner.
3. On **Choose a password**, type a password of at least 12 characters that mixes at least two kinds of characters (lower case, upper case, digits, symbols) and differs from the user name. Type it again under **Type it again** and choose **Create the organization**.

Central makes the organization, its first administrator with the role Owner, the built-in roles, the group **All computers**, and the four access profiles **Standard**, **Locked down**, **Developers** and **Monitor only**, with **Standard** as the default. The console opens with the Owner signed in.

5.3 Turn On Two-Factor Sign-In

Turn on two-factor sign-in for the Owner now, and for every other administrator when they first sign in. It needs an authenticator app that makes time-based codes, on a phone or another device of the administrator.

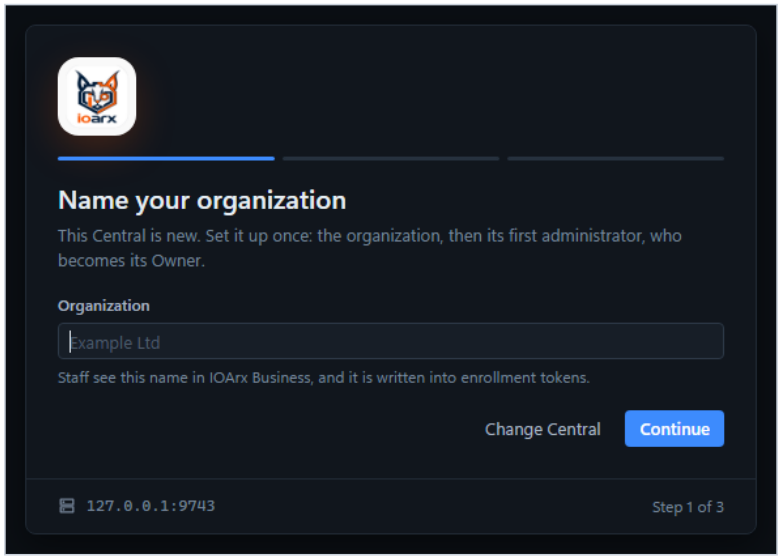


Figure 5.1: The first step of the setup of a new Central

1. Choose your name at the top right of the console, then **My account**.
2. Choose **Turn on two-factor sign-in**, type your password, and choose **Continue**.
3. Add the account to the authenticator app: enter the **Secret** as a time-based key of 6 digits every 30 seconds, or open the **Setup link** with an app that accepts it.
4. Type the code that the app shows in **Code for the new account** and choose **Turn on**.

From the next sign-in on, the console asks for the code of the app after the password. To move the account to a new phone, choose **Move to a new app** under **My account**.

5.4 Require Two-Factor Sign-In

1. Open **Settings** › **Sign-in**.
2. Turn on **Require two-factor sign-in**.
3. Under **Sign out after**, set the minutes without use after which the console locks, from 5 to 240. The default is 30.
4. Choose **Save**.

Administrators without two-factor sign-in must then turn it on at their next sign-in, before they can do anything else, and nobody can turn their own two-factor sign-in off. Every session ends after 12 hours in all, whatever the time without use.

5.5 Organization and Support Contact

Under **Settings** › **Organization**, check the **Name** of the organization and fill in **Support**: whom staff contact about IOArx, such as an e-mail address or a phone extension. The IOArx Business app shows the name as **Managed by** and the support contact as **Help**. Choose **Save**.

5.6 The Addresses of Central

Set the addresses of Central before you create the first enrollment token: every token carries them, and every new policy brings enrolled computers the current list (Section 3.5).

1. Open **Settings** › **Server**.
2. Under **Addresses of Central**, put the DNS name of Central first, such as `central.northbridge.example`. Keep IP addresses that every staff computer reaches if you want them as further choices, and remove addresses that staff computers cannot reach. Write host names or IP addresses without the port, in the order in which computers try them.
3. Choose **Save**.

The panel **Certificate** of the same tab shows the port, the subject of the certificate, the date until which it is valid, its fingerprint and its pin.

5.7 Use the Console from Another Computer

Administrators work from their own Windows computers with the console alone. It needs no service and opens no port on those computers.

1. On the computer of the administrator, run `IOArx-Central-Monitoring_1.0.0_x64-setup.exe` as in Section 4.2. When the installer asks **Should this computer run IOArx Central Monitoring for your organization?**, choose **No**. To install the console alone without a window, run as an administrator:

   Command Prompt, as an administrator, on the computer of an administrator

   ```
   IOArx-Central-Monitoring_1.0.0_x64-setup.exe /S /CONSOLE
   ```

2. Open IOArx Central Monitoring. On **Connect to IOArx Central**, under **Address of IOArx Central**, type the address of Central, such as `central.northbridge.example`, and choose **Continue**. The port is 9743 unless you add another one, as in `central.northbridge.example:9743`.
3. On **Check the fingerprint**, compare every group of the fingerprint with the fingerprint under **Settings** › **Server** on the Central computer, or with the output of `print-pin` there. Choose **The fingerprints match, connect** only if every group matches.
4. Sign in with your user name, your password and the code of your authenticator app.

From then on, the console trusts only this certificate for this address, and it lists this Central on **Connect to IOArx Central** for the next start (Figure 5.2). On the Central computer, the console offers **IOArx Central on this computer** first; **Connect to another Central** leads to the address field there.

The console of an administrator updates itself from `ioarx.com` and stays a console alone. IOArx Central updates with the console on the Central computer (Section 11.10.2).

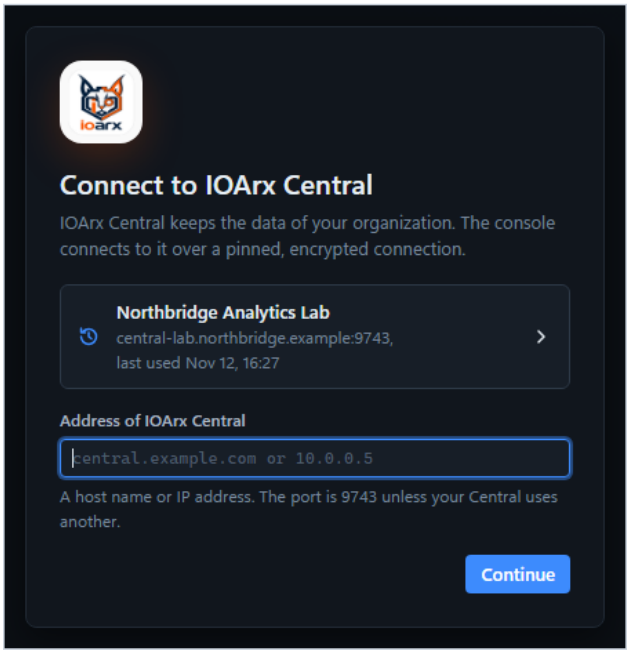


Figure 5.2: Connect to IOArx Central on the computer of an administrator, with a Central used before

5.8 Sessions, Locking and Shortcuts

The console ends sessions that stay unused, locks itself on request, and offers shortcuts for the keyboard.

Table 5.1: Sessions and shortcuts of the console

Item	How it works
Time without use	After the minutes set under **Settings** › **Sign-in**, 30 by default, the console locks and asks for the password again.
Length of a session	12 hours in all.
Lock the console	**Ctrl+L**, or **Lock the console** in the menu under your name.
Search or jump to	**Ctrl+K** opens the command palette: pages, computers, people, events, incidents by number, and actions such as **Create an enrollment token**.
Filter of a table	**/** moves to the filter of the current table; **Esc** closes a drawer.
Wrong passwords	Five wrong passwords or codes in a row lock the account for 15 minutes. Another administrator can unlock it (Section 8.4).
Closing the window	The console stays in the notification area.

5.9 The Console at a Glance

The rail on the left lists the pages in six groups (Table 5.2). It shows only the pages that the role of the administrator allows. The status bar at the bottom shows the address of Central and whether the console runs on the Central computer, the versions of Central and of the console, the state of the license with its seats, the computers online, the administrator and the scope, and the time with its

offset from UTC.

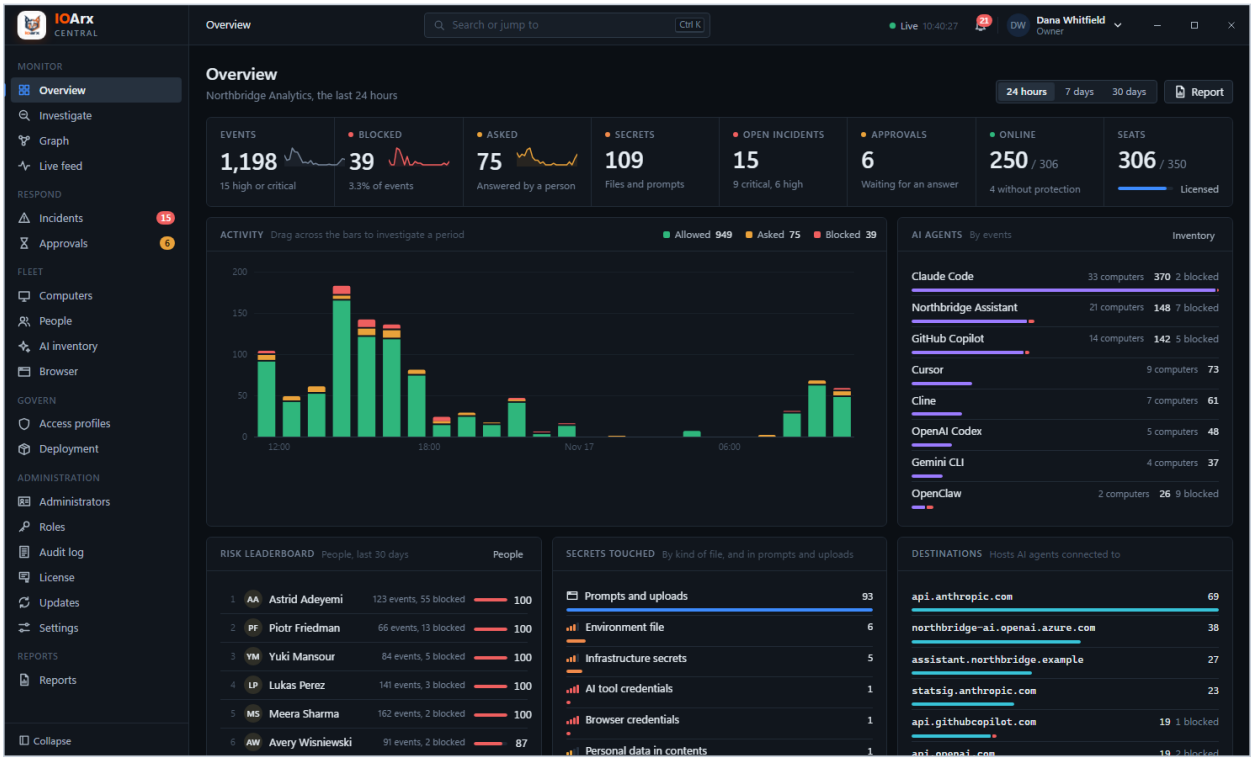


Figure 5.3: The Overview of IOArx Central Monitoring

Table 5.2: The pages of the console

Group	Pages	What you do there
Monitor	**Overview**, **Investigate**, **Graph**, **Live feed**	Watch the organization and search every event.
Respond	**Incidents**, **Approvals**	Work on incidents, answer AI agents that wait and requests for access.
Fleet	**Computers**, **People**, **AI inventory**, **Browser**	Manage computers and people, see the AI agents in use and the browser figures.
Govern	**Access profiles**, **Deployment**	Set the policy, the groups and the enrollment tokens.
Administration	**Administrators**, **Roles**, **Audit log**, **License**, **Updates**, **Settings**	Run Central itself.
Reports	**Reports**	Print a summary of a period.

CHAPTER 6

Activating the License

The license of IOArx Business covers a number of computers, its seats. Central activates the license key once with `ioarx.com`, keeps the signed license token it receives, and confirms the license every 6 hours. Staff never see a license screen: Central answers for every computer.

6.1 The Trial

Until a license is active, Central runs a trial of 14 days for up to 10 computers, counted from its first start. **License** shows the state **Trial** and the days left. When the trial ends without a license, Central refuses new enrollments, and each computer stops protecting at its next call to Central (Section 6.4).

6.2 Activate a License Key

A license key has 20 letters and digits in groups of five, such as `IOARX-XXXXX-XXXXX-XXXXX-XXXXX`. The prefix `IOARX`, spaces and hyphens are optional.

1. Sign in as an Owner. Activation needs the permission **Manage the license** and the whole organization as scope; of the built-in roles, only Owner has that permission.
2. Open **License**.
3. Under **Activate**, type the key in **License key** and choose **Activate**.

Central activates the key with `ioarx.com` and receives a signed license token with the plan, the seats and the dates. The panel **State** then shows **Licensed**, the plan, the seats in use, and the dates **Ends**, **Confirmed until**, **Grace period until** and **Last confirmed**.



Figure 6.1: A license in force, and the field for another license key

Central checks every license token with the public key of `ioarx.com` that is built into it, and only accepts a token that names this Central. A token made for another Central, or changed by one byte, is refused.

6.3 A Proxy for ioarx.com

Central reaches `ioarx.com` with the proxy settings of the system. To use another proxy:

1. Open **Settings** › **Network**.
2. Under **Proxy for ioarx.com**, type the address of the proxy, such as `http://proxy.northbridge.example:8080`. For a proxy that needs a password, write it into the address: `http://user:password@proxy.northbridge.example:8080`.
3. Choose **Save**.

Central seals the address with its key before it stores it, shows the password masked, and never writes it to a log. Leave the field empty to use the settings of the system again.

6.4 License States

Table 6.1: The states of the license

State	Meaning	Computers protect
Trial	No license key is active, and the 14 days of the trial run. Up to 10 computers.	Yes
Licensed	The license is in force, and Central has confirmed it with `ioarx.com` within the last 14 days.	Yes
Grace period	The license has expired, and the grace period of the license runs.	Yes, until the date under **Grace period until**
Expired	The license and its grace period have ended, or the trial has ended without a license.	No
No license	No license is active: it was released, `ioarx.com` reported it revoked, or Central has not confirmed it with `ioarx.com` for 14 days.	No

When the license is not in force, Central refuses new enrollments and tells each computer at its next call that its seat is not licensed. The computer then stops protecting, and its app shows **Protection is paused**. Protection starts again as soon as Central confirms the seat.

6.5 Seats

Each enrolled computer takes one seat, from its enrollment until you retire it (Section 13.1). **License** and the status bar of the console show the seats in use.

- When every seat is taken, Central refuses new enrollments with the message **Every seat of the**

license is taken. Retire computers that are gone, or add seats to the license.

- When a license covers fewer computers than are enrolled, the computers enrolled first keep their seats. The others stop protecting, and **Computers** shows them with **No seat**, until seats are freed or added.
- A computer that joins again with a new token, after its uninstall code was given or after its system was installed again, takes a second seat until you retire its earlier record (Section 13.3).

6.6 When the License Cannot Be Confirmed

Central confirms the license with `ioarx.com` every 6 hours. When `ioarx.com` cannot be reached, **License** says that the last check failed and that Central tries again every 6 hours, and the license stays in force until the date under **Confirmed until**, 14 days after the last confirmation. After that, the state turns to **No license**. Check the internet connection of the Central computer and the proxy (Section 6.3), then choose **Confirm now**.

A staff computer that cannot reach Central keeps protecting for the period under **Settings** › **Computers** › **Protect without Central for**, 30 days by default and from 1 to 90 days, counted from the last time Central confirmed its seat.

6.7 Move the License to Another Central

The activation belongs to the Central computer: the license token names an identifier of it. To use the key on another Central:

1. On the Central that holds the license, open **License**, choose **Release the activation**, type `release`, and choose **Release**. Central releases the activation with `ioarx.com`.
2. On the other Central, activate the key (Section 6.2).

After the release, the first Central has no license, unless its trial of 14 days still runs, and its computers stop protecting at their next call to it. The same applies after a restore of Central on a new computer: activate the key there (Section 11.11.1).

CHAPTER 7

Access Profiles

An access profile says what AI agents may do on the computers that follow it. It holds rules for files and folders, rules for files that hold secrets, network rules, lists of programs, the AI agents of the organization, detection, prompts, locks, the browser policy, privacy, and the behavior of IOArx Business on the computers. One profile serves Windows and Linux computers alike: each computer keeps the rules written for its own system. Section 3.8 explains which profile a computer follows.

7.1 The Four Profiles That Come Ready

Central creates four profiles at its setup. They also serve as templates for new profiles.

Table 7.1: The four profiles that come ready

Profile	What it does	Main settings
Standard, the default	AI agents ask an administrator before they use personal folders or any file that holds secrets.	Ask for every AI agent on the Documents, Desktop, Pictures and Downloads folders of every user, on Windows and Linux. Ask for every file that holds secrets. An administrator answers within 120 seconds. Browser: Warn.
Locked down	AI agents never touch files that hold secrets, ask an administrator before personal folders, and the browser blocks prompts with secrets.	Ask on the personal folders. Block for every file that holds secrets. An administrator answers within 300 seconds. Browser: Block, private windows turned off, no Open once.
Developers	Developers answer for themselves when an AI agent wants a file that holds secrets. Personal folders stay open to AI agents.	Ask for every file that holds secrets, answered by the person at the computer within 60 seconds. No rules for folders. Browser: Warn.
Monitor only	Everything AI agents do is recorded and reported. Nothing is stopped.	No rules. Browser: Warn, which lets the person send a prompt anyway.

All four profiles have behavior detection and content inspection on, install and lock IOArx for Browsers (Business), send command lines with secrets taken out and full file paths, keep tamper protection on, keep the app open, and show staff their own activity. Where no rule covers a file, they allow the access.

7.2 Create and Edit a Profile

1. Open **Access profiles** and choose **New profile**.
2. Type a **Name** and a **Description**. Under **Start from**, choose **A template** and one of the four

templates, or **A copy of a profile** and the profile to copy.

3. Choose **Create**. The editor opens on the new profile.

No computer follows a new profile until you assign it to a group, a person or a computer (Section 8.2).

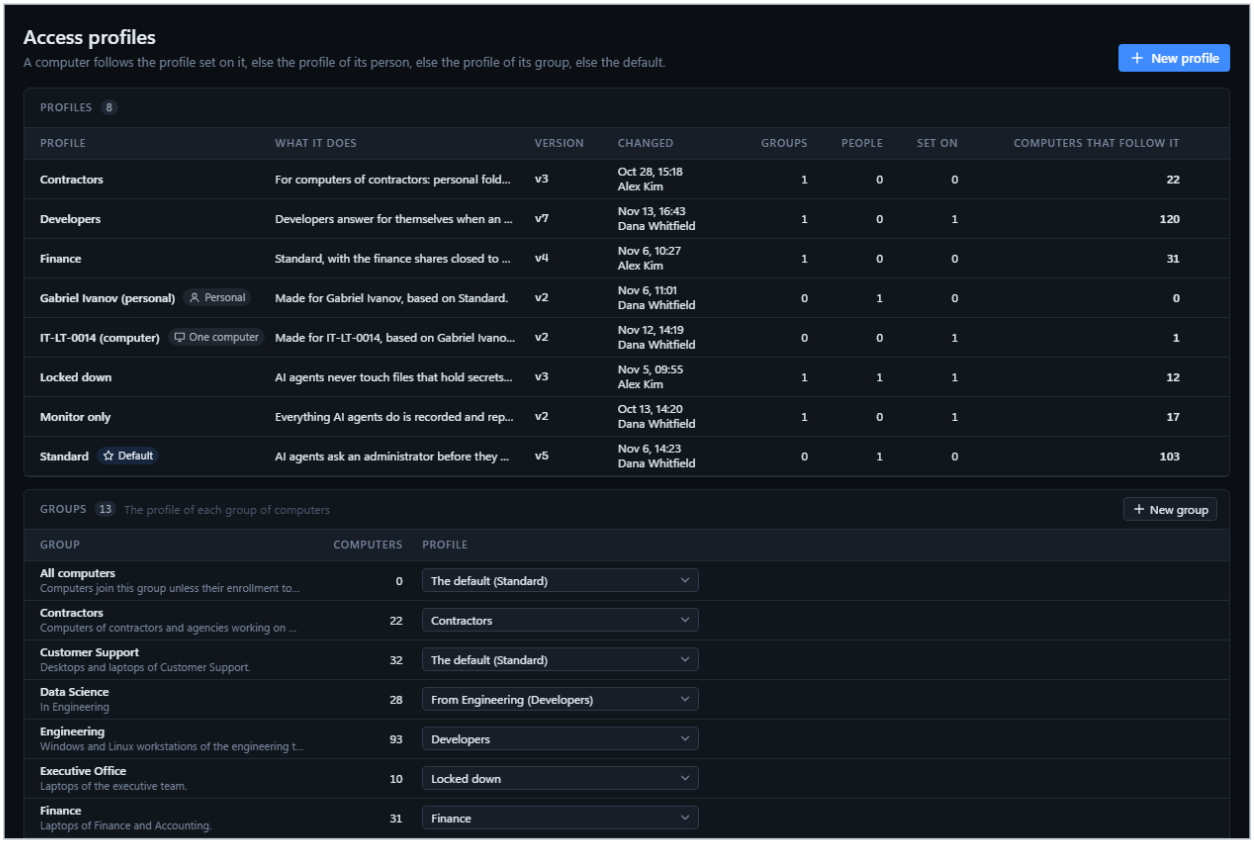


Figure 7.1: Access profiles, with the profile of each group

The editor lists the parts of the profile on its left: **Files and folders**, **Secrets**, **Network**, **Programs**, **AI agents**, **Detection**, **Prompts**, **Locks**, **Browser**, **Privacy** and **Computers**, then **Versions** and **Simulate**. Changes stay in the editor until you save them:

- A bar at the bottom names the parts you changed. **Save version** saves the profile as its next version; **Discard** drops the changes.
- Every computer that follows the profile receives the new version with its next heartbeat.
- Under **Versions**, every saved version stays, with who saved it and when. Open one to see it, or choose **Bring back into the editor** and save it as the newest version.
- When another administrator saved the profile while you edited it, the editor offers **Load version** to start again from the newest version, or **Save mine over it**.
- Central gives every rule and lock an id that no other rule of the organization has, such as `#1042`. The same id appears in the console and in the activity log of every computer.

The menu of a profile on the **Access profiles** page also offers **Duplicate**, **Make it the default**, and **Delete**. A profile can be deleted only when it is not the default and no group, person or computer uses it.

7.3 Files and Folders

A rule for a file or folder names the path, for whom it applies, which operations it covers and its action.

Table 7.2: The fields of a rule for a file or folder

Field	Value
File or folder	A full path. A folder covers everything beneath it. `*` stands for one whole folder level: `C:\Users\*\Documents` is the Documents folder of every user. Windows paths start with a drive, `C:\`, or a share, `\\server\share`; Linux paths start with `/`. Write Windows and Linux paths as separate rules; each computer keeps the rules for its system.
For	**Every AI agent**, **One AI agent** (from the catalog and the AI agents of the organization), **Any program**, or **One program** by the full path of its file.
Operations	**Read**, **Write**, **Delete**, **Rename**. All four checked: every operation.
Action	**Allow**, **Ask** or **Block**. Ask pauses the AI agent until the answer of the approver of the profile (Section 7.9).

The most specific rule wins: the longest path, then one AI agent over every AI agent, then Block over Ask over Allow. **When no rule covers a file** sets what happens to a file access of an AI agent that no rule names: **Allow**, **Ask** or **Block**. **Add the personal folders** adds Ask rules for the Documents, Desktop, Pictures and Downloads folders of every user, on Windows and Linux, where they are missing.

1. In the editor, open **Files and folders** and choose **Add a rule**.
2. Fill in **File or folder**, **For**, **Operations** and **Action**, and choose **Add the rule**.
3. Choose **Save version**.

A path holds no `.` or `..` parts, `*` stands alone for a whole folder level, and a path has at most 1,024 characters. The switch in the column **On** turns a rule off without deleting it.

7.4 Files That Hold Secrets

IOArx knows files that hold secrets by their path and by what they hold. One rule covers every SSH key, cloud credential, password database and the rest, wherever they are. A rule about secrets beats a rule for the folder the file is in; a rule for the file itself beats both.

Table 7.3: The fields of a rule about secrets

Field	Value
For	**Every AI agent**, **One AI agent**, **Any program** or **One program**.
Action	**Allow**, **Ask** or **Block**.
Inside	A folder to which the rule is limited. Empty: anywhere on the computer.
Kinds of secret	**Every kind**, or the kinds you check (Table 7.4).

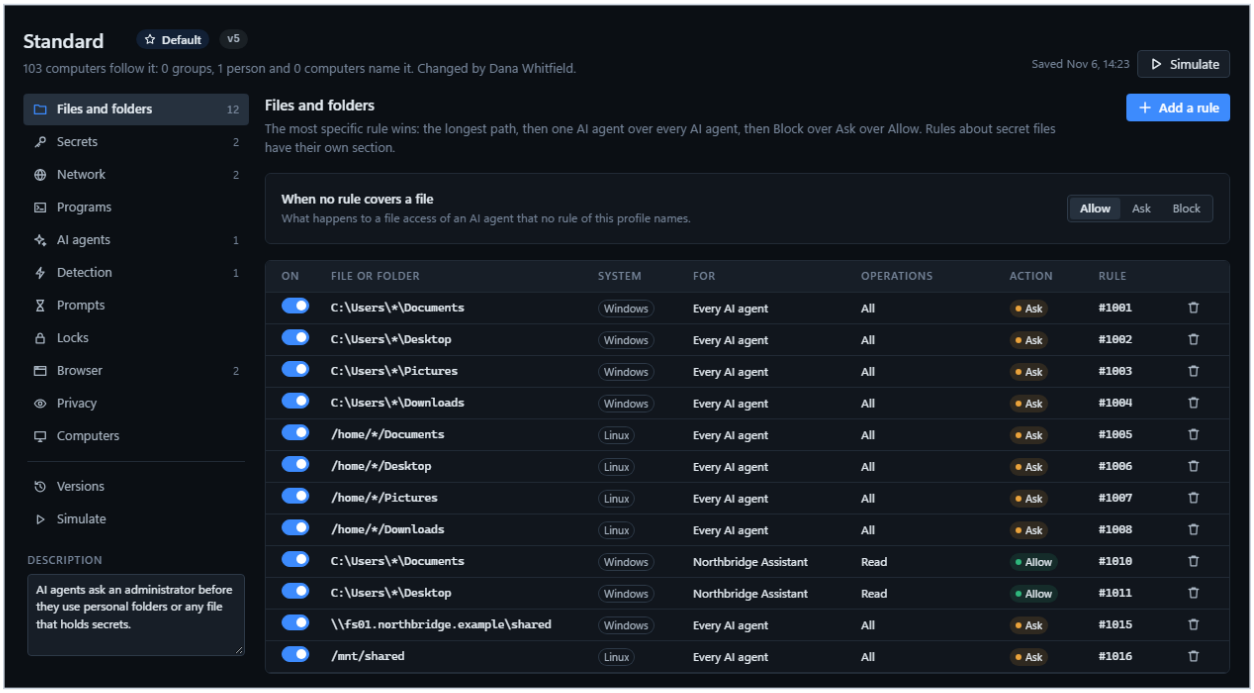


Figure 7.2: Rules for files and folders of the profile Standard

Table 7.4: The kinds of secret

Kinds of secret that IOArx recognizes			
SSH key	Private key	Cloud credentials	Environment file
Password database	Browser credentials	Access token	Secrets file
AI tool credentials	Crypto wallet	System credentials	Remote access profile
Database credentials	Chat app session	Command history	Infrastructure secrets
Email archive	Personal document	Secret in contents	Personal data in contents

The last two kinds come from content inspection, which reads files whose names say nothing about what they hold (Section 7.8).

7.5 Network Rules for AI Agents

Network rules decide which hosts AI agents may connect to. They follow an AI agent into every program it starts, such as `curl` or a shell.

Table 7.5: The fields of a network rule

Field	Value
For	**Every AI agent** or **One AI agent**.
Destinations	Up to 500 destinations (Table 7.6). No destination: every destination outside the computer.

Field	Value
Action	**Allow**, **Ask** or **Block**.

Table 7.6: How to write destinations

Destination	Covers
`api.example.com`	That host.
`*.example.com`	The domain and every host under it.
`203.0.113.7`	One address.
`10.0.0.0/8`	A network.
`api.example.com:443`	A host, an address or a network on one port.

The rule that names the other end most narrowly wins, then one AI agent over every AI agent, then the strictest action. Without a rule, a connection is allowed. Connections within the computer are always allowed.

7.6 Programs

The two lists of **Programs** apply to every program of the computer, not only to AI agents, before a connection is made. The blocked list wins over the allowed list.

- **Programs whose connections are blocked**: full paths of program files, such as `C:\Tools\uploader.exe`.
- **Ask mode**: only the **Allowed programs** may start network connections. Every other program is refused until an answer allows it.

> **Important.** Ask mode covers every program of the computer. List every program that needs the network, such as the browsers, the mail client and the tools of the organization, under **Allowed programs** before you turn it on.

7.7 AI Agents of Your Organization

IOArx Business recognizes the AI agents of its built-in catalog, which comes with each version; the editor lists it under **The built-in catalog**. Add the AI agents that your organization builds or uses and that the catalog does not know.

1. In the editor, open **AI agents** and choose **Add an AI agent**.
2. Type the **Name** and the **Vendor**, and choose the **Kind**: Coding agent, AI editor, Assistant, Local models, Autonomous agent, Agentic browser, or Automation. An entry with the name of a built-in AI agent adds its ways of recognition to that agent.
3. Under **Recognized by any of these**, add one or more ways (Table 7.7), with **Add a way to recognize it**.
4. Choose **Save version**.

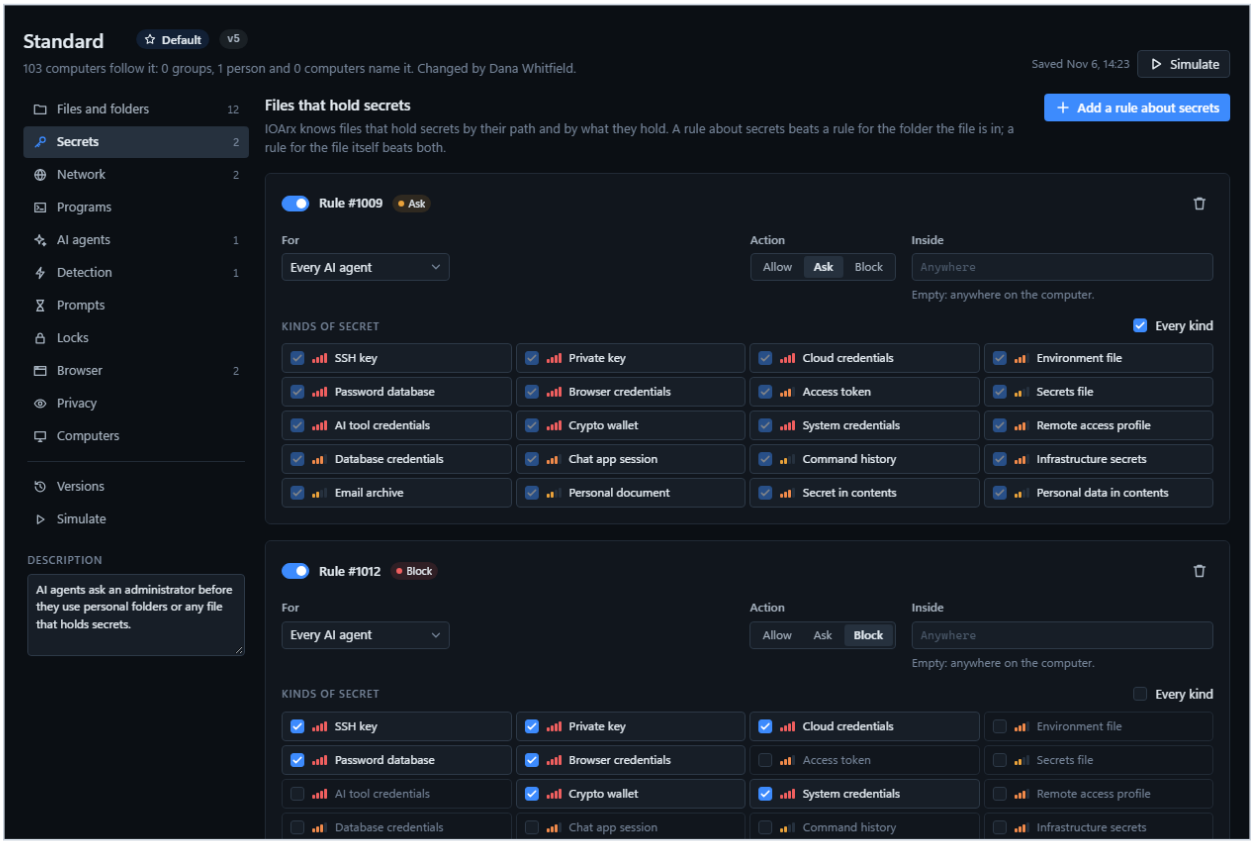


Figure 7.3: Rules about secrets: Ask for every kind, and Block for the most sensitive kinds

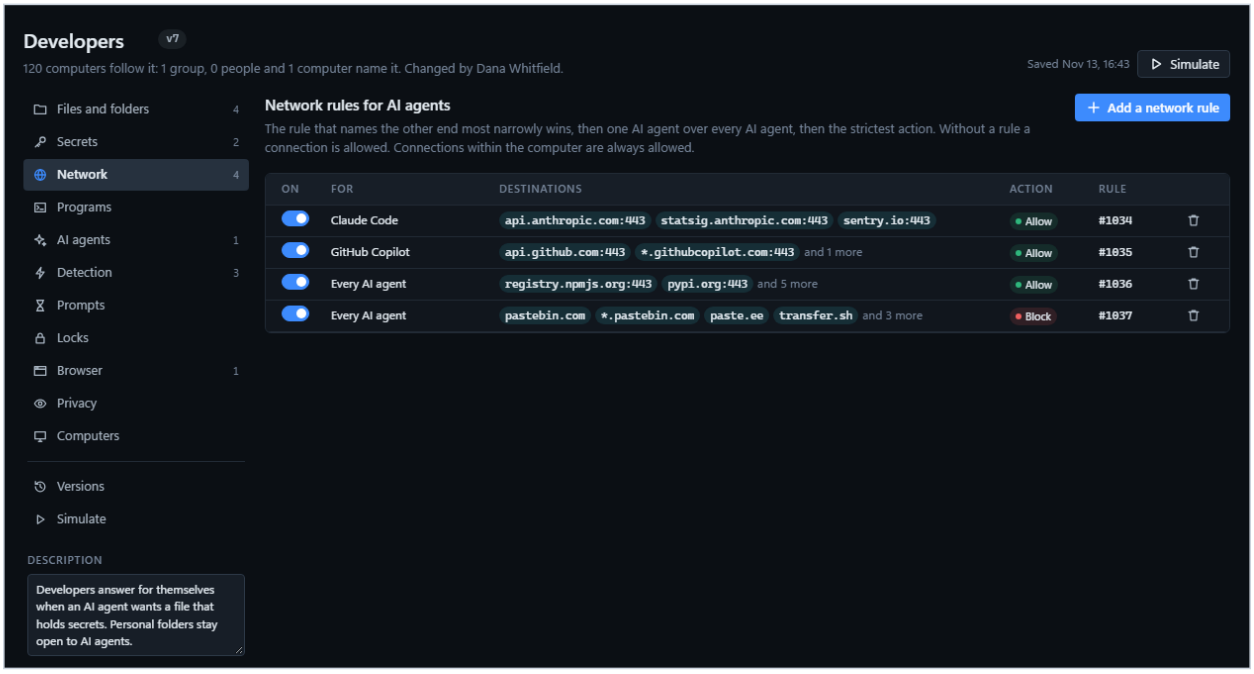


Figure 7.4: Network rules of the profile Developers: the hosts that Claude Code, GitHub Copilot and every AI agent need are allowed, paste services are blocked

Table 7.7: Ways to recognize an AI agent

Way	Example	Evidence
Signed by	The publisher, such as Acme Ltd, and optionally the product	Verified
App package	`Acme.Copilot_8wekyb3d8bbwe`	Verified
Program file name	`acme-agent.exe`	Unverified
Text in the program path	`acme-agent`	Unverified
Text in the command line	`acme-agent`	Unverified
Environment variable	`ACME_AGENT_SESSION`	Unverified

A signature or an app package is verified evidence. A file name, a folder or text in the command line can be imitated by another program. A profile adds at most 200 AI agents, each with 1 to 50 ways of recognition.

7.8 Detection

- **Behavior detection** watches programs for the behavior of an AI agent, such as a model service, an agent loop or the keys of AI services, and treats a program it finds like a known AI agent. Under **Programs behavior detection leaves alone**, list programs by the full path of their file.
- **Content inspection** reads the files that an AI agent opens, when their path tells nothing, for secrets and personal data. Only the kind and the number of findings are kept, never the text.

7.9 Prompts

Prompts sets who answers when a rule says Ask, and how long the AI agent waits, paused, for the answer.

Table 7.8: Who answers when a rule says Ask

Who answers	What happens
An administrator	The request appears on the **Approvals** page at once. The AI agent waits, paused, and the person at the computer sees that it waits for an administrator.
The person at the computer	IOArx Business asks the person in its app, as IOArx Personal does.
Nobody	Ask counts as Block. Use it where nobody can answer in time.

Time to answer is from 10 seconds to one hour. When it runs out, the AI agent is stopped, as if the answer were Block.

7.10 Locks

A lock keeps every program of a signed-in person out of a file or folder, on every computer that follows the profile, until an administrator removes the lock. On Windows, the locked file or folder

gets an access list for SYSTEM and administrators only, with an entry for OWNER RIGHTS that keeps its owner from writing the list back. On Linux, it belongs to root with mode 0700 for a folder or 0600 for a file. Removing the lock restores exactly the access that was there before.

1. In the editor, open **Locks**.
2. Type the path under **File or folder**, such as `C:\Users\*\Documents\Payroll` or `/srv/finance/payroll.xlsx`, and the reason under **Why**, then choose **Lock**.
3. Choose **Save version**.

SYSTEM and the administrators of a Windows computer, and root on Linux, keep access to a locked file or folder. Central refuses locks that would stop the computer itself, and every computer checks again against its own folders:

- a whole drive, the folder of Windows, `Program Files`, `Program Files (x86)` and `ProgramData` as a whole;
- `C:\Users`, a user folder as a whole, and the `AppData` folder of a user as a whole;
- files on other computers, such as `\\server\share\finance`: lock them on those computers;
- on Linux, `/` and every folder at its top level as a whole, the system folders such as `/etc`, `/usr` and `/boot` with everything in them, and a home folder as a whole;
- the folders of IOArx Business.

Locks of a profile apply on every computer that follows it. To lock a file or folder on one computer, use the page of the computer (Section 11.6). A profile holds at most 200 locks.

7.11 Browser

Browser sets what IOArx for Browsers (Business) does on AI services in Chrome, Edge and Firefox. Chapter 10 describes its deployment.

Table 7.9: The browser settings of a profile

Setting	What it does
Install and lock the extension	IOArx for Browsers (Business) is installed by browser policy and cannot be turned off or removed.
Turn off private windows	Incognito, InPrivate and Firefox private windows are turned off, so that no prompt escapes the extension.
When a prompt holds a secret	**Warn**: the person may send it anyway, which is reported. **Block**: the findings must be removed first.
Check pasted text	Looks at text when it is pasted into a prompt.
Check files before upload	Looks into files before they are uploaded to an AI service.
Hints while typing	Shows a hint next to the prompt while it holds a secret.
Open once	Offers to open a blocked AI service once, which is reported.
Report AI service use	Reports which AI services the browsers of the computer reach, from their name lookups, hour by hour.

The table of AI services sets, for each service, **Prompts**: **As the mode says**, **Not checked**, **Warn** or

Block, and **Cannot be opened**, which blocks the service altogether. The table of detectors turns each detector of the extension on or off for the profile, with its default under **By default**.

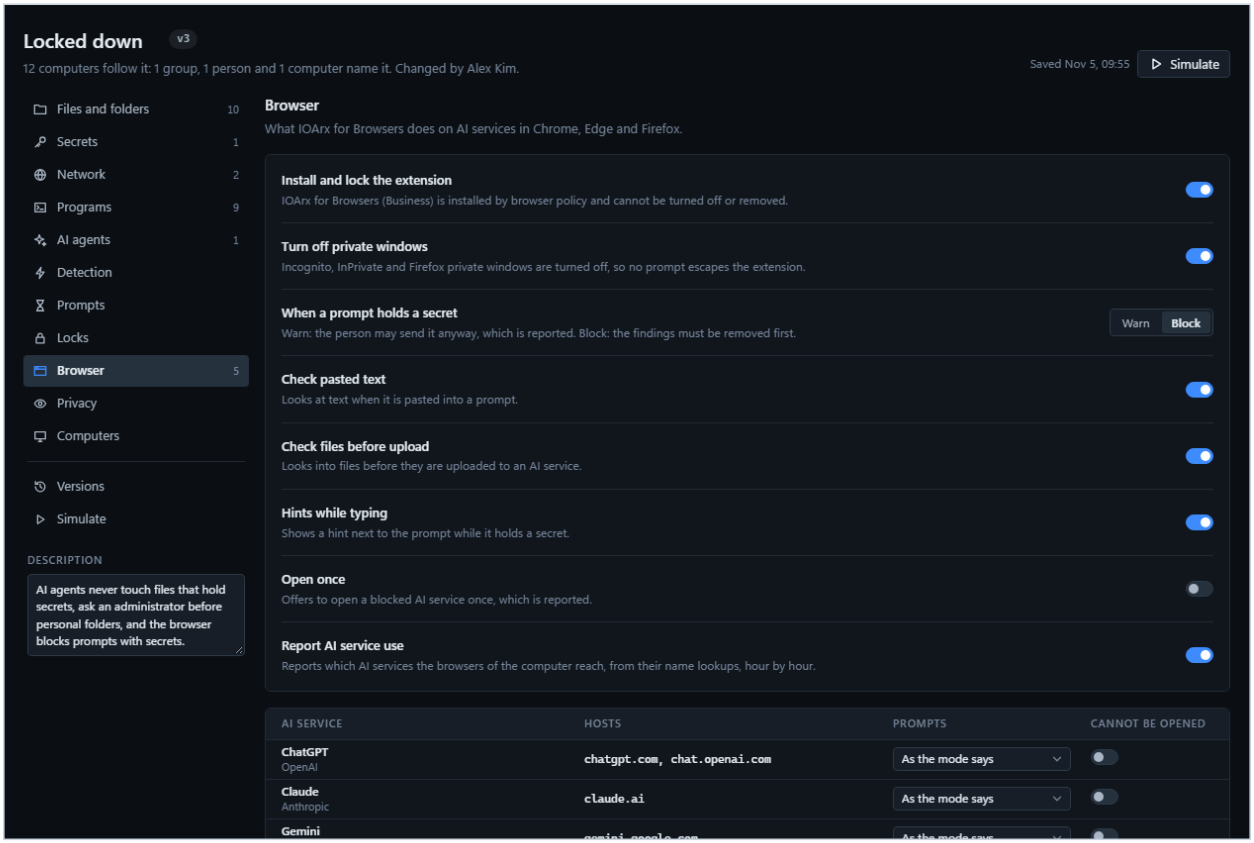


Figure 7.5: The browser settings of the profile Locked down

7.12 Privacy

- **Command lines**: **With secrets taken out**, where every secret that the detectors find is replaced by its kind; **Only the program**, where the arguments stay on the computer; or **Not at all**.
- **File paths**: **Full paths**, or **Only the folder**, where file names stay on the computer.
- **Privacy notice for staff**: the notice that staff read in IOArx Business, up to 20,000 characters. Leave it empty for the built-in notice.

7.13 Computers

Table 7.10: How IOArx Business behaves on the computers of a profile

Setting	What it does
Tamper protection	The service cannot be stopped or uninstalled without an administrator of Central (Section 12.2). On by default.

Setting	What it does
Staff may close the app	Lets staff quit the app. Protection goes on either way; the app only shows it. Off by default.
Staff see their own activity	The app shows each person what is reported about them. On by default.
Notify when an AI agent is stopped	Staff get a notification when IOArx stops an AI agent. On by default.

How often computers call in is set once for every computer, under **Settings** › **Computers** › **Heartbeat**: 30 seconds by default, from 10 to 600 seconds.

7.14 Limits of a Profile

Table 7.11: Limits of one access profile

Item	Limit
Rules for files, folders and secrets	2,000
Network rules	1,000
Destinations of one network rule	500
Locks	200
Entries of each list of programs	1,000
AI agents of the organization	200, each with 1 to 50 ways of recognition
Time to answer	10 seconds to one hour
Privacy notice	20,000 characters
Length of a path	1,024 characters

7.15 Simulate

Simulate shows what the engine of IOArx decides for a request under the saved version of a profile, without any computer involved.

1. In the editor, choose **Simulate**.
2. Choose the **System**, **Windows** or **Linux**, the **Operation**, and under **By** an AI agent or **A program that is not an AI agent**.
3. Type the **File**, or for **Connect** the **Host**, the **Address** and the **Port**. Optionally, type the **Program** file, for rules about one program.
4. Choose **Simulate**.

The **Outcome** is Allow, Ask or Block, with an explanation, the rule that decided it or **No rule; the default applied**, and for Ask, who answers. The simulation uses the saved version of the profile; save your changes first to include them.

CHAPTER 8

Groups, People, Administrators and Roles

8.1 Groups

Every computer belongs to one group: the group of the enrollment token it used, until an administrator moves it. Groups can sit inside other groups. A group follows a profile of its own; a group without one follows the nearest group above it that has a profile, else the default profile of the organization. **Access profiles** shows such a group with the group and profile it follows, such as **From Engineering (Developers)**. The group **All computers** exists from the setup and cannot be deleted.

1. Open **Access profiles**. The panel **Groups** lists every group with its computers and its profile.
2. Choose **New group**. Type the **Name**, choose under **Inside** either **Top level** or the group above, type a **Description**, and choose the **Access profile**: a profile of its own, or the first choice, which follows the group above it or the default.
3. Choose **Create**.

To give an existing group another profile, choose the profile in the row of the group. Its computers follow the new profile from their next heartbeat. Choosing the profile of a group needs the permissions **Manage computers** and **Change access profiles**.

To move a computer to another group, open its page under **Computers**, then **Settings**, choose the **Group**, and choose **Save**. A group can be deleted only when it holds no computers; enrollment tokens that put computers into it can no longer be used afterwards.

8.2 Profiles for a Person or a Computer

- **For a person:** under **People**, open the person, choose **Edit**, and choose an **Own access profile**. It wins over the profile of the groups of the person's computers. **From the group** removes it.
- **For one computer:** under **Computers**, open the computer, then **Settings**, and choose an **Access profile**. Set on the computer, it wins over the profile of its person and of its group. **Inherit from the person or the group** removes it.
- **As the default:** on **Access profiles**, open the menu of a profile and choose **Make it the default**. Computers whose computer, person and group name no profile follow it from their next heartbeat.

The page of a computer shows under **Policy** which profile it follows, where it comes from (**Set on the computer**, **From the person**, **From the group** or **Organization default**), the version, and whether the computer has applied it. Answers to approval requests and requests for access can create profiles for one computer or one person automatically (Section 11.3).

8.3 People

People are the staff to whom computers belong. A person has a name, an e-mail address, a department, which is one of the groups, the accounts they sign in with, and optionally a profile of their own.

When **Make people from accounts** is on under **Settings** › **Retention and privacy**, as it is by default, an account that a computer reports and that no person lists makes a new person, named after the account, in no department. One computer makes at most 20 people a day this way. A computer without a person is linked to the person of an account it reports only if that person uses no other computer and has no profile of their own; an administrator makes every other link, under the **Settings** of the computer.

1. Open **People** and choose **Add a person**.
2. Type the **Name** and the **Email**, choose the **Department** and, if needed, an **Own access profile**.
3. Under **Accounts**, add the accounts the person signs in with, such as `NORTHBRIDGE\mmorgan` on Windows or `mmorgan` on Linux.
4. Choose **Add**.

The risk score of a person, from 0 to 100, sums the events of the last 30 days: 1 for each low, 3 for each medium, 10 for each high and 25 for each critical event, halved for every 7 days of age. When pseudonyms are on, changing the accounts of a person needs the permission **See the names behind pseudonyms**. Deleting a person keeps the events of their computers, which then lose the link to the person.

8.4 Administrators

1. Open **Administrators** and choose **Add an administrator**.
2. Type the **Name**, **User name** and **Email**.
3. Choose the **Role**. Under **Scope**, choose **The whole organization**, or **Some groups** and check the groups.
4. Type a **First password** of at least 12 characters with at least two kinds of characters, and keep **Ask for a new password at the first sign-in** on.
5. Choose **Add**, and give the administrator their user name and first password over a separate, trusted channel.

The menu of an administrator offers **Edit**, **Set a new password**, **Unlock** for an account that wrong passwords locked, **Turn off two-factor sign-in** for an administrator who lost their phone, **Disable** or **Enable**, and **Delete**. A new password ends every session of that administrator. Only an Owner gives or takes the Owner role, the last active Owner keeps it and stays enabled, and nobody deletes their own account. The audit log keeps what a deleted administrator did.

An administrator whose scope is a list of groups sees and manages only the computers of those groups, the people assigned to those computers, and their events, incidents and approval requests. Activating the license, making backups and changing the settings of Central need the whole organization as scope.

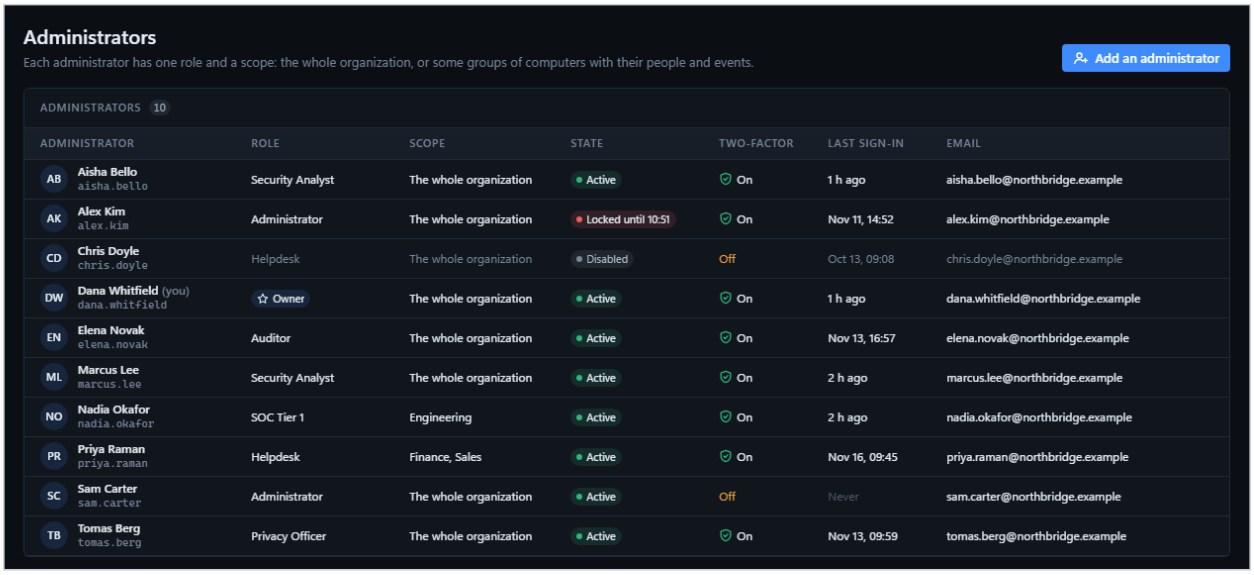


Figure 8.1: Administrators with their roles, scopes and two-factor sign-in

8.5 Roles

The page **Roles** shows the permissions of every role as a table; Appendix D lists them. The built-in roles keep their permissions. To give a set of permissions a name of its own:

1. Open **Roles** and choose **New role**.
2. Type the **Name**, such as SOC Tier 1, and a **Description**, and check the permissions.
3. Choose **Create**.

Change the permissions of a role of your own in its column of the table and choose **Save**; administrators with the role have the new permissions from their next request. A role can be deleted only when no administrator holds it.

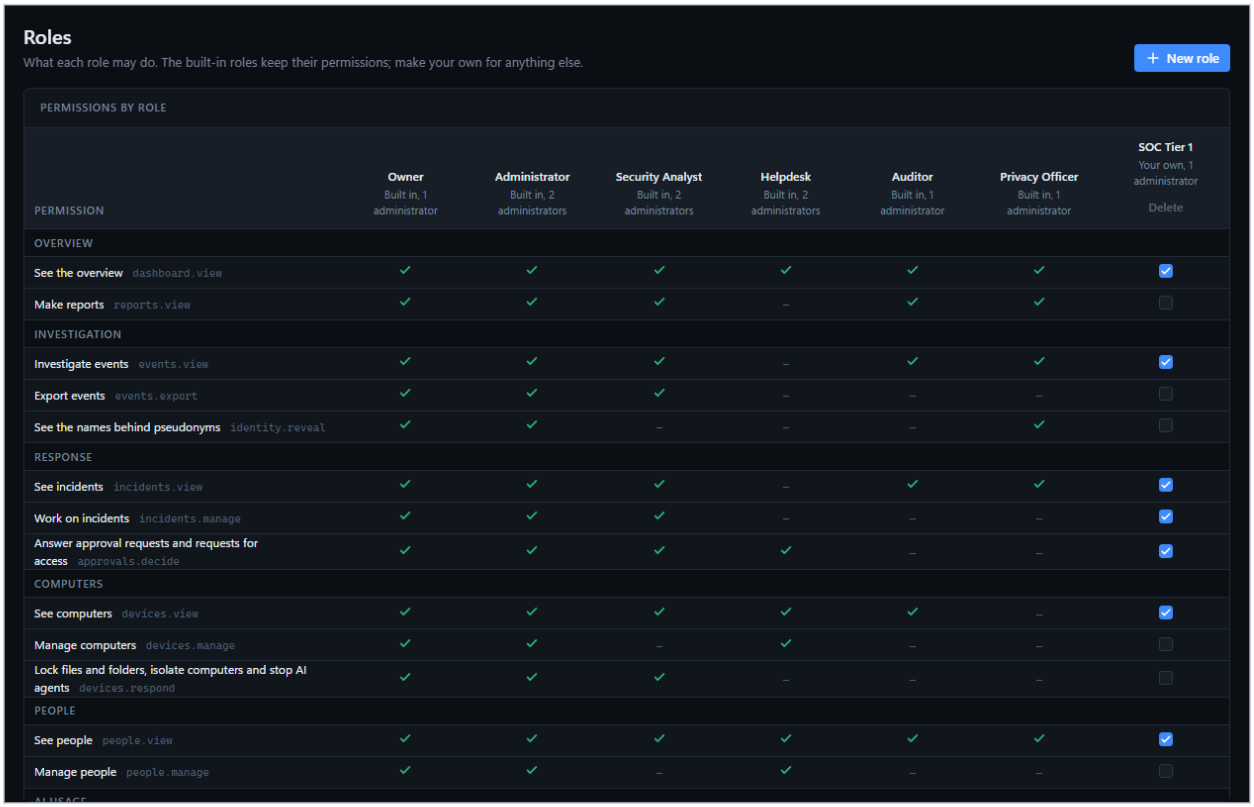


Figure 8.2: Permissions by role, with a role of the organization in the last column

CHAPTER 9

Deploying IOArx Business

Every staff computer joins Central with an enrollment token, which the installer passes to the service of IOArx Business. This chapter creates tokens, then installs IOArx Business interactively, silently, with Microsoft Intune, Group Policy, Configuration Manager, and on Linux, and shows how to check that each computer has joined.

9.1 Before You Deploy

- The license has a free seat for every computer, or the trial covers the pilot (Chapter 6).
- The addresses of Central are set under **Settings** › **Server** (Section 5.6).
- The groups and their profiles are ready (Chapters 7 and 8).
- The store ids of IOArx for Browsers (Business) are entered under **Settings** › **Browser extension** (Section 10.2). The four profiles that come ready install the extension; without the store ids, Chrome and Edge get no extension.
- On Windows, IOArx Personal is uninstalled from the computers that will run IOArx Business. On Linux, the package of IOArx Business replaces it (Section 9.12).
- The staff computers reach Central on TCP port 9743 (Section 3.4).

9.2 Enrollment Tokens

An enrollment token lets computers join one group of the organization, for a limited time and, if you choose, for a limited number of computers. Create one token for each group and each rollout.

1. Open **Deployment** and choose **Create an enrollment token**.
2. Type a **Name**, such as Main office rollout.
3. Under **Computers join the group**, choose the group of the new computers.
4. Under **Valid for**, choose 1 day, 7 days, 30 days, 90 days or 1 year.
5. Under **Uses**, type the number of computers that may join with the token, or leave it empty for no limit.
6. Choose **Create**. **Your enrollment token** shows the token and the install commands for Windows and Linux with the token in them.
7. Copy the token and keep it where your deployment tools read it, then choose **Done**.

> **Important.** Central shows a token once, when it is created. It keeps only a hash of the token and cannot show it again. The install commands of the **Deployment** page carry the token until you leave the page.

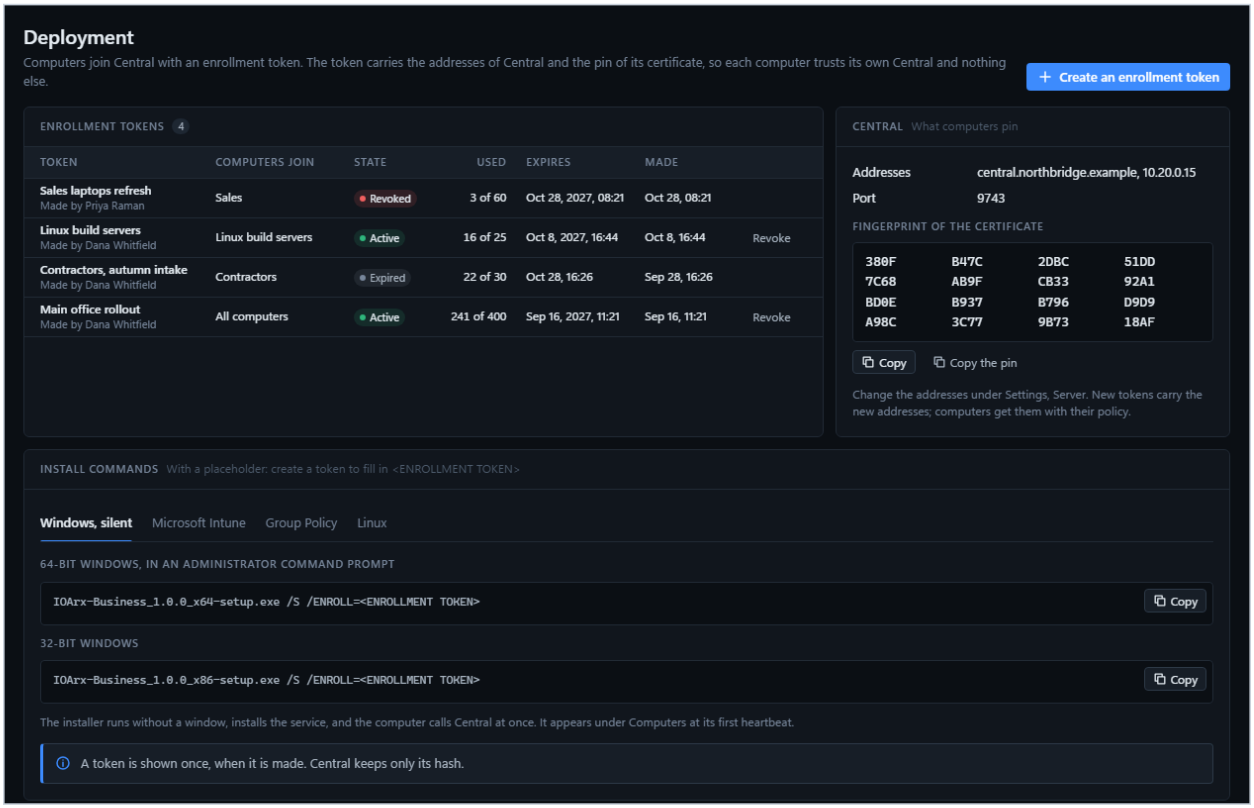


Figure 9.1: Enrollment tokens, the addresses and fingerprint that computers pin, and the install commands

Table 9.1: States of an enrollment token

State	Meaning
Active	Computers can join with the token.
Used up	As many computers as the token allows have joined with it.
Expired	The token is older than its validity.
Revoked	An administrator revoked the token.

To revoke a token, choose **Revoke** in its row, then **Revoke the token**. No computer can join with it any more; computers that joined with it stay enrolled.

Keep tokens as you keep passwords. A valid token lets any computer join the organization and take a seat. It cannot take over a computer that Central knows: every enrollment makes a new record (Section 13.3). Give tokens a short validity and a limited number of uses, and revoke them when the rollout is complete.

9.3 Get the Installers

Five minutes after its first start, and every 12 hours after that, Central downloads the newest packages of IOArx Business from `ioarx.com` and checks their signatures. The panel **Packages of IOArx Business** of the **Deployment** page lists the newest package for each system; **Download**

saves a copy. The same files are at https://ioarx.com/updates/business/. Check the code signature of each Windows installer before you distribute it:

PowerShell

```
Get-AuthenticodeSignature .\IOArx-Business_1.0.0_x64-setup.exe
Get-AuthenticodeSignature .\IOArx-Business_1.0.0_x86-setup.exe
```

The column `Status` shows `Valid` for each file.

9.4 How Enrollment Works

Figure 9.2 shows what happens between the token and the first heartbeat. The computer reaches Central only over TLS to the certificate whose pin the token carries, so a token cannot lead a computer to another server.

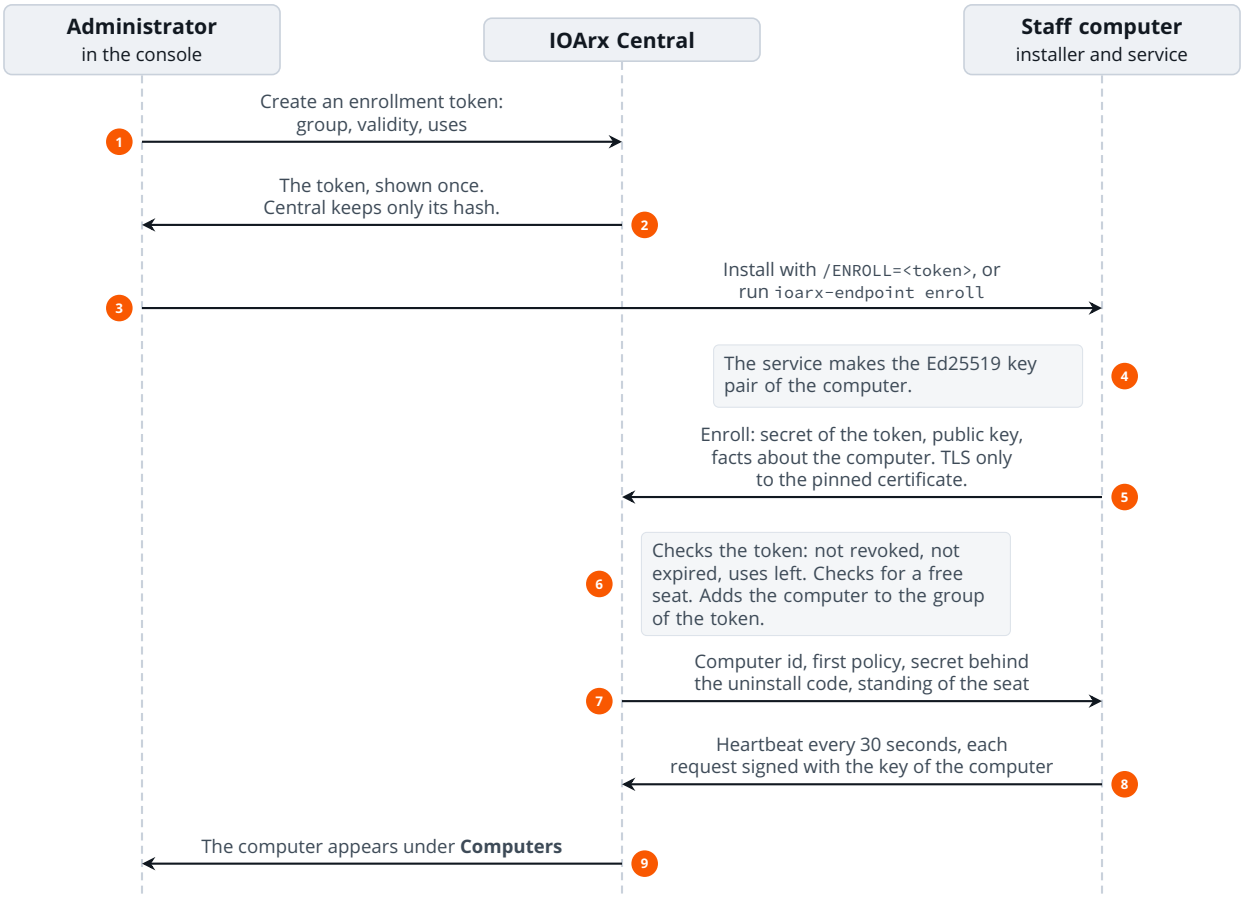


Figure 9.2: Enrollment of a staff computer

9.5 Install on One Windows Computer

Use the window of the installer on single computers, such as the first computers of a pilot.

1. Copy `IOArx-Business_1.0.0_x64-setup.exe` to the computer. On 32-bit Windows, use `IOArx-Business_1.0.0_x86-setup.exe`.
2. Open a Command Prompt as an administrator in the folder of the installer, and run the installer with the token:

   Command Prompt, as an administrator

   ```
   IOArx-Business_1.0.0_x64-setup.exe /ENROLL=<enrollment token>
   ```

3. On **Welcome to IOArx Business Setup**, choose **Next**.
4. On **License Agreement**, read the license agreement and choose **I Agree**.
5. On **Choose Install Location**, keep `C:\Program Files\IOArx Business` and choose **Next**.
6. On **Choose Start Menu Folder**, keep the folder `IOArx Business` and choose **Install**.
7. Wait until the installer has finished, then choose **Finish**.

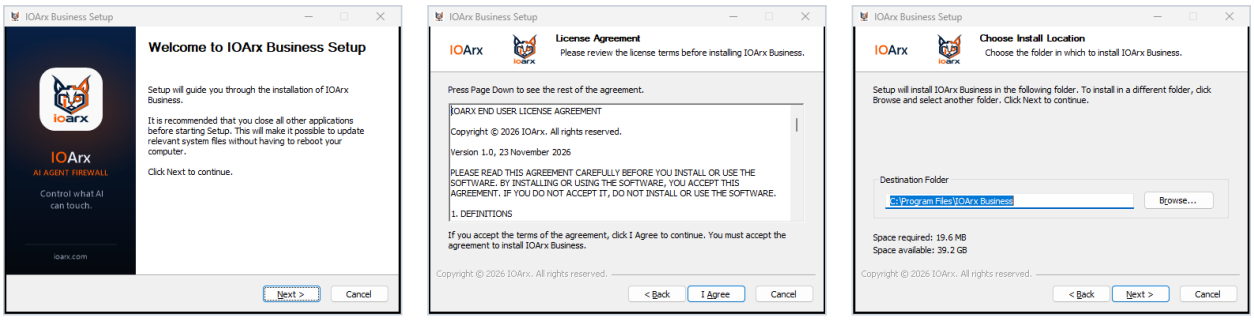


Figure 9.3: The installer of IOArx Business: Welcome, License Agreement and Choose Install Location

The computer calls Central at once and appears under **Computers** within a minute. An installer run without `/ENROLL` installs IOArx Business without joining Central (Section 9.11).

9.6 Silent Installation on Windows

The silent installation runs without a window. Run it as an administrator, or as SYSTEM from a management tool:

Command Prompt, as an administrator or as SYSTEM

```
IOArx-Business_1.0.0_x64-setup.exe /S /ENROLL=<enrollment token>
```

The installer installs the service, and the computer calls Central at once. It appears under **Computers** at its first heartbeat.

Table 9.2: Options of the installer of IOArx Business

Option	Meaning
`/S`	Installs without a window. Creates the shortcuts in the Start menu and on the desktop.

Option	Meaning
`/ENROLL=<token>`	The enrollment token. The installer leaves it for the service, which enrolls at its start.
`/NS`	Creates no shortcuts in the Start menu or on the desktop. The app still starts at every sign-in.
`/CODE=<uninstall code>`	The uninstall code of the computer, for an installation over an existing one started by hand, and for removal (Section 13.2).

Table 9.3: Exit codes of the installer

Exit code	Meaning
`0`	Installed.
`5`	IOArx Business is already installed and managed by Central, and refused the installation because the uninstall code was missing or wrong.

The uninstaller, `uninstall.exe`, copies itself to the temporary folder of Windows, starts the copy and returns at once, so its exit code does not tell whether IOArx Business was removed. Section 13.2 shows how to check the removal.

> **Note.** Update IOArx Business through Central (Section 11.10). An installer that you start by hand on a computer that runs IOArx Business stops with exit code 5, unless you give it the uninstall code of that computer with `/CODE=`.

9.7 What the Installer Does on Windows

Table 9.4: What the installer of IOArx Business sets up

Item	Details
Programs	`C:\Program Files\IOArx Business`: the app `IOArx Business.exe`, the service `ioarx-endpoint.exe`, and `uninstall.exe`.
Enrollment	The installer runs `ioarx-endpoint.exe enroll` with the token, which writes the token to `C:\ProgramData\IOArx Business\enroll.json`. The service enrolls at its start and deletes the file once it has enrolled.
Service	`IOArxBusiness`, display name IOArx Business, as LocalSystem, with automatic start. After a failure, Windows starts it again after 5 seconds. With tamper protection on, only LocalSystem may stop, pause, reconfigure or delete it.
Start at sign-in	The value `IOArx Business` of `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`: `"C:\Program Files\IOArx Business\IOArx Business.exe" --background`.
Data folder	`C:\ProgramData\IOArx Business`, open to SYSTEM and administrators only.
Browsers	The native messaging host and, when the profile installs the extension, the browser policies (Chapter 10).
Start menu	The folder `IOArx Business`, with the app.

9.8 Microsoft Intune

Deploy IOArx Business with Microsoft Intune as a Windows app (Win32).

1. Put `IOArx-Business_1.0.0_x64-setup.exe` alone in a folder, such as `C:\Packages\IOArx`, and wrap it with the Microsoft Win32 Content Prep Tool:

   Command Prompt

   ```
   IntuneWinAppUtil.exe -c C:\Packages\IOArx -s IOArx-Business_1.0.0_x64-setup.exe -o
       ↪ C:\Packages\Output
   ```

2. In the Microsoft Intune admin center, add an app of the type **Windows app (Win32)** and upload the `.intunewin` file from `C:\Packages\Output`.
3. On **Program**, enter the settings of Table 9.5.
4. On **Requirements**, choose the 64-bit architecture and Windows 10 as the minimum version.
5. On **Detection rules**, configure a rule manually with the settings of Table 9.5.
6. On **Assignments**, assign the app as required to the device groups that join Central.

Table 9.5: Settings of the Win32 app in Microsoft Intune

Setting	Value
Install command	`IOArx-Business_1.0.0_x64-setup.exe /S /ENROLL=<enrollment token>`
Uninstall command	`"C:\Program Files\IOArx Business\uninstall.exe" /S`
Install behavior	System
Device restart behavior	No specific action
Detection rule type	File
Path	`C:\Program Files\IOArx Business`
File or folder	`IOArx Business.exe`
Detection method	File or folder exists

For 32-bit Windows, add a second app with `IOArx-Business_1.0.0_x86-setup.exe` and the 32-bit architecture as its requirement.

> **Important.** Intune needs an uninstall command, but every computer has an uninstall code of its own, so no single command carries it. The command of Table 9.5 removes IOArx Business only from a computer that Central has retired, or whose profile turns tamper protection off. On every other computer, the uninstaller refuses, IOArx Business stays installed, and Central records an attempt to uninstall without the code, which opens an incident. To remove IOArx Business, retire the computer in the console: IOArx Business then removes itself (Section 13.1).

Before you retire a computer that Intune manages, remove it from the assignment of the app. Otherwise Intune installs IOArx Business on it again with the token of the install command, and the retired computer joins again as a new computer with a seat of its own (Section 13.3).

9.9 Group Policy

With Group Policy, a computer startup script installs IOArx Business where it is missing. The **Deployment** page shows this script under **Group Policy**, with the share you type and the token you created.

1. Copy `IOArx-Business_1.0.0_x64-setup.exe` to a shared folder that the computer accounts can read, such as `\\fs01.northbridge.example\deploy\ioarx`. Give the group Domain Computers read access to the share and to the folder.
2. Save the script as `install-ioarx.ps1`:

   install-ioarx.ps1

   ```
   # IOArx Business: installs at computer startup when it is not installed yet.
   # Group Policy: Computer Configuration, Policies, Windows Settings, Scripts, Startup.
   $installer =
       ↪ "\\fs01.northbridge.example\deploy\ioarx\IOArx-Business_1.0.0_x64-setup.exe"
   if (-not (Test-Path "$env:ProgramFiles\IOArx Business\IOArx Business.exe")) {
     Start-Process -FilePath $installer -ArgumentList '/S', '/ENROLL=<enrollment token>'
       ↪ -Wait
   }
   ```

3. In Group Policy Management, edit a Group Policy Object that is linked to the organizational units of the computers. Under **Computer Configuration** › **Policies** › **Windows Settings** › **Scripts (Startup/Shutdown)**, open **Startup**, and add `install-ioarx.ps1` on the tab **PowerShell Scripts**.
4. Restart a computer of the organizational unit and check that it appears under **Computers**.

The script runs at every start of a computer and installs IOArx Business only where it is missing. It installs the 64-bit package: give 32-bit computers a Group Policy Object of their own with the x86 installer. When the token expires or you revoke it, put a new token into the script.

9.10 Configuration Manager and Other Tools

In Microsoft Configuration Manager, create an application with a deployment type for a script installer:

- Installation program: `IOArx-Business_1.0.0_x64-setup.exe /S /ENROLL=<enrollment token>`.
- Installation behavior: install for system.
- Detection method: the file `C:\Program Files\IOArx Business\IOArx Business.exe` exists.

Any other software distribution tool runs the same silent command as SYSTEM or as an administrator. The uninstall command and the note of Section 9.8 apply to every tool.

9.11 Install Now, Enroll Later

IOArx Business can be installed without a token, for example in a standard image. From its first start, the service protects the computer for 72 hours with the profile Standard, which the person at the

computer answers, since no administrator can be asked yet. If the computer has not enrolled after 72 hours, protection pauses until it enrolls. To enroll it, run as an administrator:

Command Prompt, as an administrator

```
"C:\Program Files\IOArx Business\ioarx-endpoint.exe" enroll --token <enrollment token>
```

Linux, as root

```
sudo ioarx-endpoint enroll --token <enrollment token>
```

The command answers `This computer joins Northbridge Analytics now.` When the service does not run at that moment, it answers that the token is saved and that the computer joins when the service starts. A computer that has enrolled keeps its identity: a token left on it is ignored, so that nobody can move it to another Central. Only after Central retired it, or after its uninstall code was given, does a new token make it join as a new computer (Section 13.3).

9.12 Linux

Install the package with the package manager of the distribution, then enroll the computer. The package manager installs the libraries that the package depends on.

Ubuntu 22.04 or later, Debian 12 or later and the distributions built on them

```
sudo apt install ./ioarx-business_1.0.0_amd64.deb
sudo ioarx-endpoint enroll --token <enrollment token>
```

Fedora

```
sudo dnf install ./ioarx-business-1.0.0-1.x86_64.rpm
sudo ioarx-endpoint enroll --token <enrollment token>
```

openSUSE Tumbleweed

```
sudo zypper install --allow-unsigned-rpm ./ioarx-business-1.0.0-1.x86_64.rpm
sudo ioarx-endpoint enroll --token <enrollment token>
```

zypper checks the rpm signature of every package. The package of IOArx Business carries the update signature of IOArx, not an rpm key, so zypper needs the option `--allow-unsigned-rpm` to install it.

9.12.1 Computers with IOArx Personal

The package of IOArx Business replaces the package of IOArx Personal, `ioarx`. apt removes it by itself. dnf needs the option `--allowerasing`. zypper asks how to resolve the conflict, or takes `--force-resolution` when it runs without questions:

Fedora, with IOArx Personal

```
sudo dnf install --allowerasing ./ioarx-business-1.0.0-1.x86_64.rpm
```

openSUSE Tumbleweed, with IOArx Personal, without questions

```
sudo zypper --non-interactive install --allow-unsigned-rpm --force-resolution
    ↪ ./ioarx-business-1.0.0-1.x86_64.rpm
```

Then enroll the computer as above.

The services `ioarx-monitor` and `ioarx-business` start at once and at every boot, and the app starts at every sign-in to a desktop session. Check the services with:

Linux

```
systemctl status ioarx-monitor ioarx-business
```

9.12.2 Enrollment through configuration management

Tools such as Ansible, Puppet or Salt write the token to `/etc/ioarx-business/enroll.token` before they install the package. The package then enrolls the computer with the token and deletes the file:

Linux, as root

```
sudo install -d -m 700 /etc/ioarx-business
sudo sh -c 'umask 077; echo "<enrollment token>" > /etc/ioarx-business/enroll.token'
sudo apt install ./ioarx-business_1.0.0_amd64.deb
```

9.12.3 What the packages install

Table 9.6: What the Linux packages of IOArx Business install

Path	What it is
`/usr/lib/ioarx-business/ioarx-endpoint`	The service. `/usr/bin/ioarx-endpoint` links to it, for administrators.
`/usr/lib/ioarx/ioarx-monitor`	IOArx Monitor.
`/usr/bin/ioarx-business`	The app.
`/usr/lib/systemd/system/ioarx-business.service`	The systemd unit of the service.
`/usr/lib/systemd/system/ioarx-monitor.service`	The systemd unit of IOArx Monitor.
`/etc/xdg/autostart/ioarx-business.desktop`	Starts the app at every sign-in to a desktop session.
`/var/lib/ioarx-business`	The data of the service, open to root only.
`/run/ioarx-business.sock`	The socket through which the app and the browsers talk to the service.

IOArx Monitor keeps its firewall rules in the nftables table `inet ioarx`, which goes away when the monitor stops.

9.13 Check Enrollment in the Console

A computer appears under **Computers** at its first heartbeat, within a minute of its installation. Check its row:

- **State** shows **Online**: the computer called in within its last three heartbeats.
- **Protection** shows **Protected**. Otherwise it shows **No seat**, **Files off** or **Network off**, and the page of the computer gives the reason (Section 14.5).
- **Policy** shows the version of the policy. An amber version means that the computer has not applied the newest policy yet.
- **Log** shows **Intact**: the chain of the activity log holds.

The chips above the table count the computers in each state: **Online**, **Without protection**, **Isolated**, **Outdated**, **Offline over 7 days**, **Signs of tampering** and **Policy not applied** (Figure 9.4). Open a computer to see its page (Figure 9.5): what protects it, the profile it follows and where the profile comes from, its activity log, its identity and, for administrators who manage computers, its uninstall code.

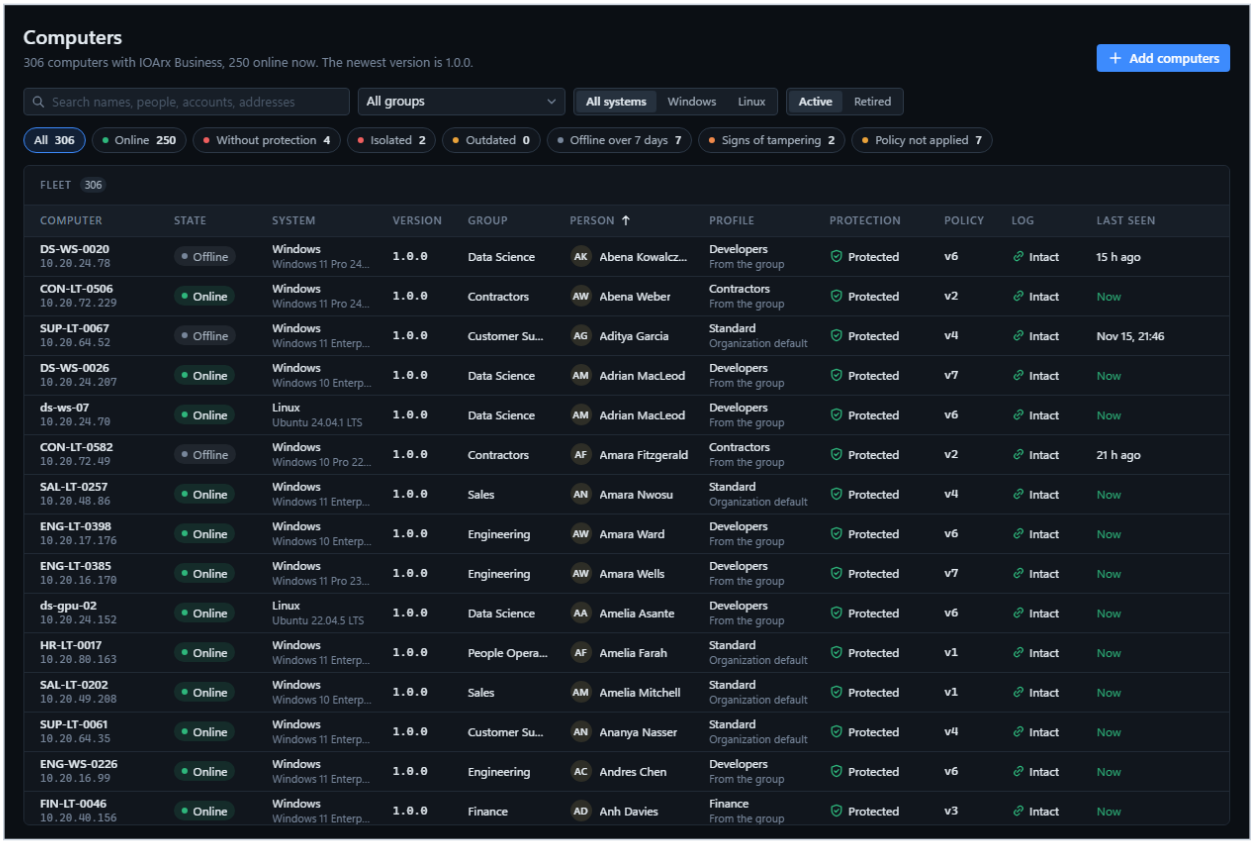


Figure 9.4: Computers, with the chips that count the computers in each state

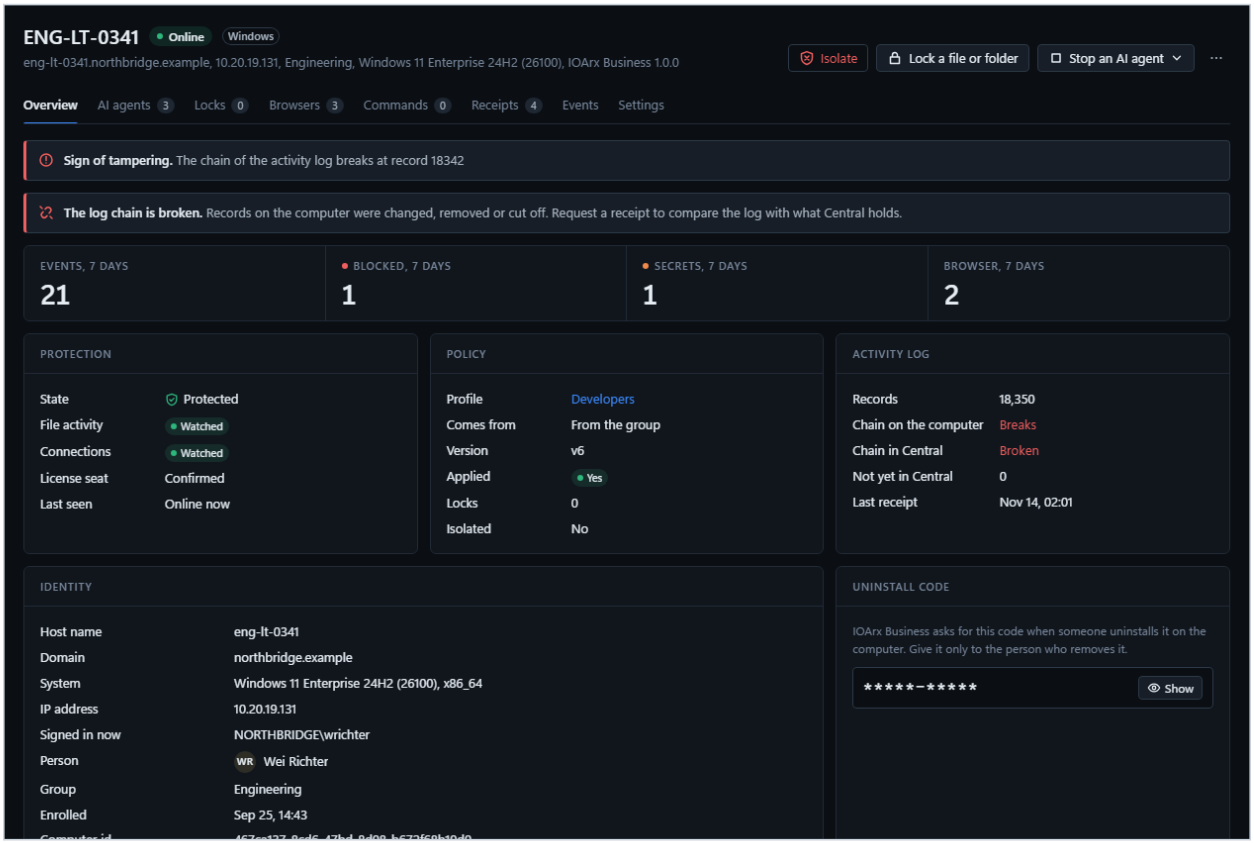


Figure 9.5: The page of a computer, here with a broken log chain that Central reports as a sign of tampering

9.14 Check Enrollment on the Computer

Command Prompt, on a Windows staff computer

```
sc query IOArxBusiness
"C:\Program Files\IOArx Business\ioarx-endpoint.exe" status
```

Linux

```
systemctl status ioarx-business ioarx-monitor
ioarx-endpoint status
```

`status` prints what the service reports, as JSON. Check these fields:

Table 9.7: Fields of ioarx-endpoint status

Field	Meaning
`enrolled`	`true` once the computer has joined Central.
`connected`	`true` while Central answers.
`central`	The address of Central in use.
`protection.monitoring`	`true` while file activity of AI agents is watched.

Field	Meaning
`protection.network`	`true` while connections of AI agents are watched.
`licensed`	`true` while Central confirms the seat of the computer.
`protection.note`	Why part of the protection is off, in words. Empty when everything runs.
`profile`, `policy_version`	The profile and the version of the policy that the computer enforces.
`approver`	Who answers when a rule says Ask: `administrator`, `employee` or `nobody`.

The page **About** of the IOArx Business app shows the same facts for staff and helpdesk: the version, the computer id, the addresses of Central, the data folder, the records sent to Central and those waiting to be sent, the chain of hashes of the activity log, and the last problem.

9.15 What Staff See

The IOArx Business app runs in the notification area of every person who signs in. Its rail has two groups, **Protection** and **Organization**.

Table 9.8: The pages of the IOArx Business app

Page	What it shows
Overview	Whether the computer is protected, the actions of the person's AI agents today, what was stopped, the secrets touched, the alerts that wait, the organization, the profile, who answers alerts, and the connection to Central with the support contact as **Help**.
Alerts	AI agents that are paused until someone answers. The person answers with **Allow** or **Block** when the profile lets them; otherwise the alert shows that it waits for an administrator.
Activity	What the person's AI agents did and what the rules decided, when the profile shows staff their own activity.
AI agents	The AI agents of the person that run now.
Requests	The requests the person sent to administrators and their answers, and the form **Ask for access**.
Rules	The profile that the computer follows, its rules, who answers alerts and the time to answer, detection, the browser policy, and the locked files and folders.
Privacy	The notice of the organization, what is collected and what is never collected.
About	The version and the state of the service, for support.

The first time the app opens, the **Overview** asks the person to read the privacy notice of the organization, which they confirm with **I have read this notice** on the page **Privacy** (Figure 9.7). When an AI agent of the person waits for an administrator, the person gets a notification that it waits; when IOArx stops an AI agent, the person gets a notification if the profile says so. The page **Rules** (Figure 9.6) shows staff what their profile lets AI agents do.

9.15.1 Requests for access

Staff ask their administrators ahead of time to let an AI agent use a file, a folder or a host, on the page **Requests** (Figure 9.8):

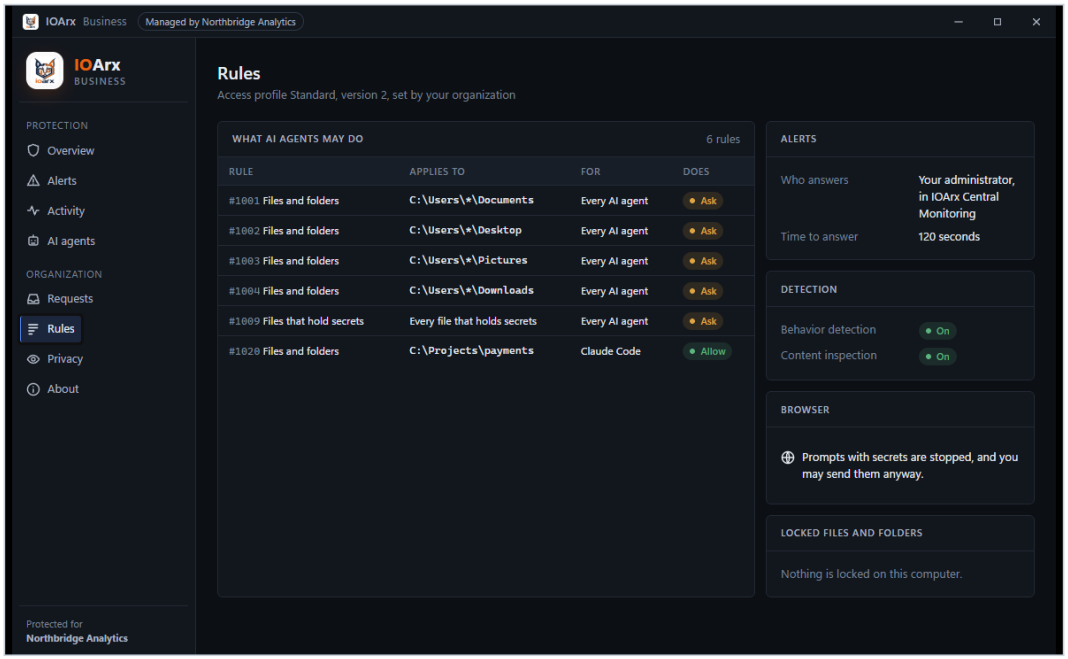


Figure 9.6: The page Rules of the IOArx Business app: the profile Standard and what it lets AI agents do

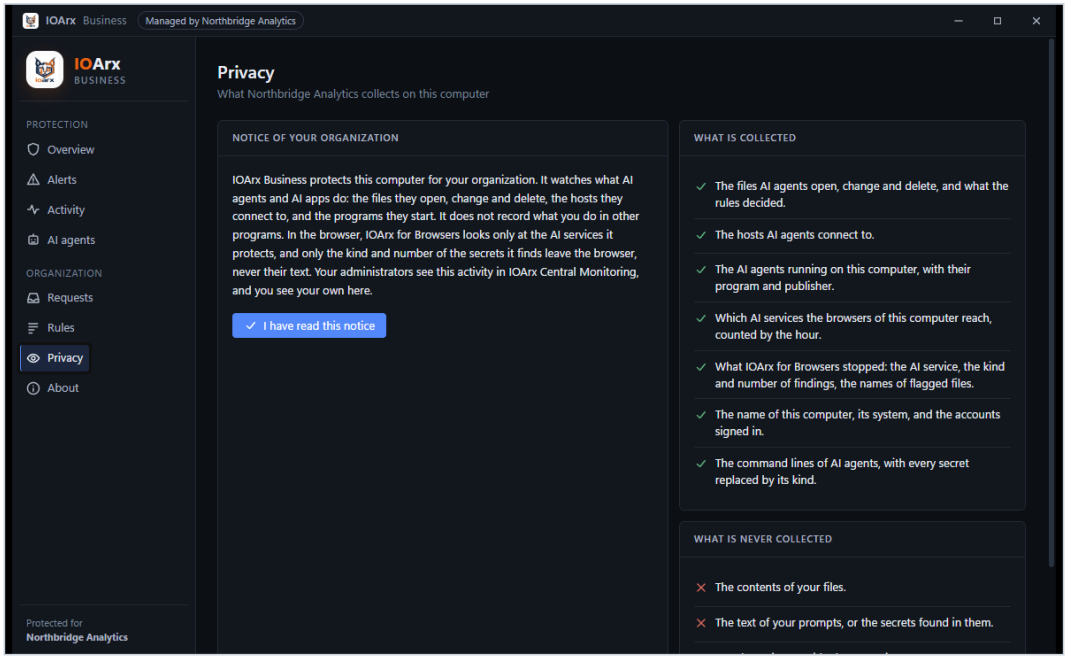


Figure 9.7: The page Privacy of the IOArx Business app, with the notice of the organization

1. Under **AI agent**, type the name of the AI agent, such as Claude Code.
2. Under **File, folder or host**, type the path or the host, such as `C:\Projects\payments` or `api.example.com`.
3. For a file or folder, choose **Read only** or **Read and change**. Read and change also lets the AI agent write, rename and delete there.
4. Under **Why**, write what the AI agent needs it for, and choose **Send request**.

A request for access waits up to 7 days for an answer, which administrators give on the page **Approvals** (Section 11.3). The list **Your requests** shows each request as **Waiting to be sent**, **Waiting for an administrator**, **Approved**, **Declined** or **Expired**.

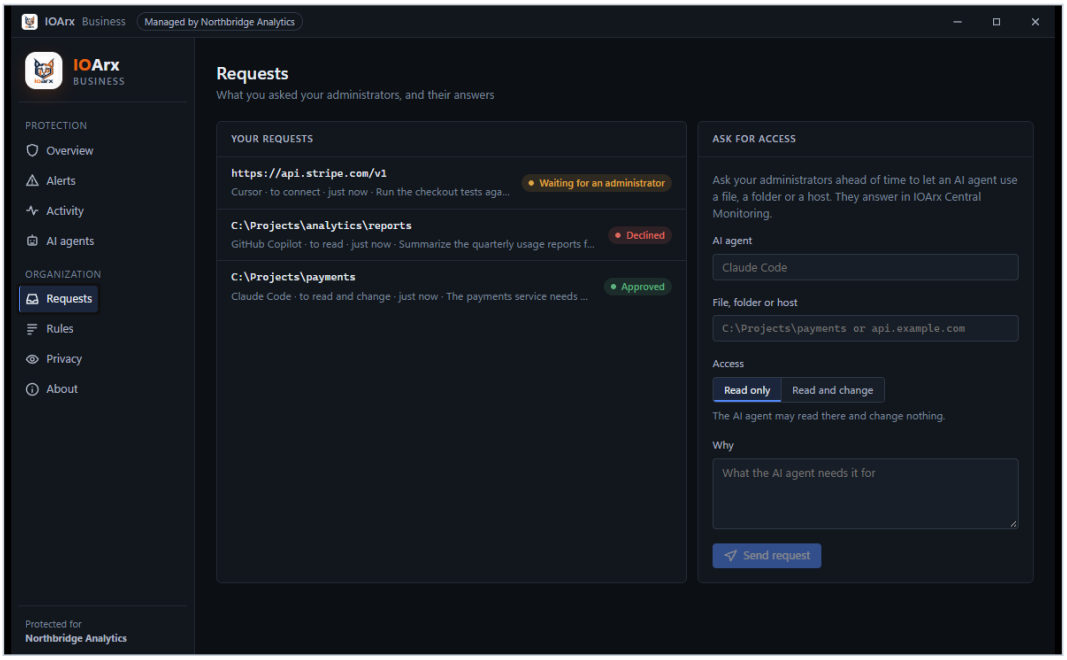


Figure 9.8: The page Requests of the IOArx Business app: three requests for access with their answers, and the form Ask for access

CHAPTER 10

Deploying IOArx for Browsers

IOArx for Browsers (Business) checks prompts, pastes and uploads on AI services in the browser, and keeps API keys, passwords and personal data from reaching them as the access profile sets. It takes its settings from the profile of the computer and reports what it stops to IOArx Business on the same computer, which forwards it to Central. Only the kind and number of findings leave the browser, never the text. IOArx Business installs the extension by browser policy, so that staff cannot turn it off or remove it.

10.1 How the Extension Is Managed

- IOArx Business registers itself with Chrome, Edge and Firefox as the native messaging host `com.ioarx.business`, and lets only the extensions with the store ids of the organization connect to it.
- When the profile has **Install and lock the extension** on, IOArx Business writes the browser policies that install the extension and keep it installed, and gives it the name of the organization and its settings before it first connects.
- When the browser starts, the extension connects to IOArx Business, receives the browser settings of the profile, and sends each event of its activity log: the time, the AI service, the kind and number of findings, the names of flagged files, and the decision.
- When the profile turns private windows off, IOArx Business sets the policies that turn off Incognito windows of Chrome, InPrivate windows of Edge and private windows of Firefox.
- IOArx Business adds its entries next to the policies of the organization, and removes exactly the entries it wrote when the profile changes or when IOArx Business is removed.

10.2 Enter the Store Ids

Chrome and Edge install IOArx for Browsers (Business) from their stores by its store id, a string of 32 letters.

1. Open **Settings** › **Browser extension**.
2. Under **Chrome**, add the id of IOArx for Browsers (Business) in the Chrome Web Store. Under **Edge**, add its id in Microsoft Edge Add-ons.
3. Leave **Firefox** empty: IOArx Business always lets `business@ioarx.com`, the id of the extension in Firefox, connect.
4. Choose **Save**.

Computers receive the ids with their next policy. Then choose the browser settings of each profile (Section 7.11).

10.3 What IOArx Business Writes on Windows

Table 10.1: Registry keys that IOArx Business writes for the browsers

Key under HKEY_LOCAL_MACHINE	What it holds
`SOFTWARE\Google\Chrome\NativeMessagingHosts\com.ioarx.business`, the same under `SOFTWARE\Microsoft\Edge`	The path of the manifest of the native messaging host, `C:\Program Files\IOArx Business\browser\chromium.json`.
`SOFTWARE\Mozilla\NativeMessagingHosts\com.ioarx.business`	The path of `browser\firefox.json`.
`SOFTWARE\Policies\Google\Chrome\NativeMessagingAllowlist`, the same for Edge	`com.ioarx.business`, so that a policy that blocks native messaging hosts still lets this one through.
`SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist`	`<Chrome id>;https://clients2.google.com/service/update2/crx`
`SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallForcelist`	`<Edge id>;https://edge.microsoft.com/extensionwebstorebase/v1/crx`
`SOFTWARE\Policies\Google\Chrome\3rdparty\extensions\<Chrome id>\policy`, the same for Edge	The values `organization` and `settings`: the settings of the extension.
`SOFTWARE\Policies\Mozilla\Firefox`	`ExtensionSettings`, which installs `business@ioarx.com` from the package of IOArx Business (Section 10.5), and `3rdparty\Extensions\business@ioarx.com` with the settings.
`SOFTWARE\Policies\Google\Chrome`, `...\Microsoft\Edge`, `...\Mozilla\Firefox`	With private windows turned off: `IncognitoModeAvailability` = 1, `InPrivateModeAvailability` = 1, `DisablePrivateBrowsing` = 1.

IOArx Business adds its entries to the lists under numbers of its own and keeps the entries of the organization. Where Group Policy of your organization also sets `ExtensionInstallForcelist` for Chrome or Edge, include the entry of IOArx for Browsers (Business) in that policy as well, so that both write the same list.

10.4 What IOArx Business Writes on Linux

Table 10.2: Files that IOArx Business writes for the browsers on Linux

File	What it holds
`native-messaging-hosts/com.ioarx.business.json` in `/etc/opt/chrome`, `/etc/chromium`, `/etc/brave` and `/etc/opt/edge`	The manifest of the native messaging host.
`policies/managed/ioarx-business.json` in the same folders	The install list, the settings of the extension, the native messaging allowlist and, when the profile says so, private windows turned off.

File	What it holds
`/usr/lib/mozilla/native-messaging-hosts/com.ioarx.business.json`, and the same under `/usr/lib64`	The manifest of the native messaging host for Firefox.
`/etc/firefox/policies/policies.json`	The policies of Firefox, written only when the file is missing or was written by IOArx Business.

Firefox reads one policies file. When your organization already has its own `/etc/firefox/policies/policies.json`, IOArx Business leaves it as it is; add the entry of IOArx for Browsers (Business) to it:

/etc/firefox/policies/policies.json

```
{
  "policies": {
    "ExtensionSettings": {
      "business@ioarx.com": {
        "installation_mode": "force_installed",
        "install_url": "file:///usr/lib/ioarx-business/extension/ioarx-business.xpi",
        "private_browsing": true
      }
    }
  }
}
```

10.5 Firefox

Firefox installs IOArx for Browsers (Business) from a package signed by Mozilla, `ioarx-business.xpi`, in the folder `extension` of the install folder of IOArx Business: `C:\Program Files\IOArx Business\extension\ioarx-business.xpi` on Windows and `/usr/lib/ioarx-business/extension/ioarx-business.xpi` on Linux. IOArx Business writes the Firefox policy that installs the extension only when that file is present; it registers the native messaging host of Firefox in every case. Firefox then installs the extension at its next start and lets it run in private windows.

Before you count on IOArx for Browsers (Business) in Firefox, check that the package is present on a staff computer:

PowerShell

```
Test-Path "C:\Program Files\IOArx Business\extension\ioarx-business.xpi"
```

Linux

```
ls -l /usr/lib/ioarx-business/extension/ioarx-business.xpi
```

The tab **Browsers** of the computer in the console lists Firefox once the extension has connected from it.

10.6 Private Windows

Extensions do not run in Incognito and InPrivate windows unless the person allows them, and Chrome and Edge have no policy that allows them. To keep prompts from going around the extension, turn on **Turn off private windows** in the profile. The profile **Locked down** does this.

10.7 Check the Coverage

The page **Browser**, titled **Browser security**, shows what IOArx for Browsers stopped, by AI service and by kind of finding, which AI services the browsers of the organization reach, and under **Extension coverage** how many computers run the extension, for each browser. On the page of a computer, the tab **Browsers** lists each browser and account with **Connected** or **Not connected**, the version of the extension, and when it last connected. A browser appears there once the extension has connected from it.

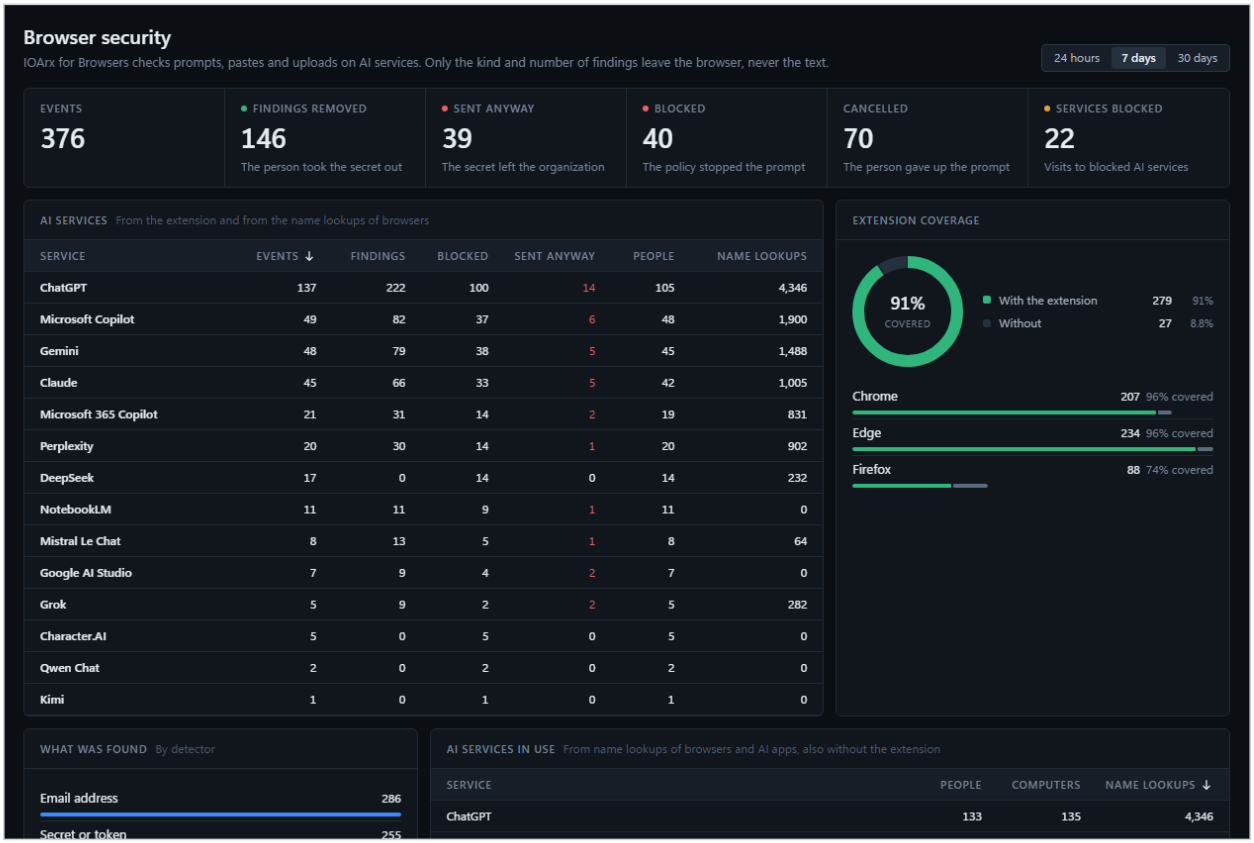


Figure 10.1: Browser security, with the coverage of the extension by browser

CHAPTER 11

Daily Operations

This chapter covers the work of the security team once IOArx Business runs: approval requests and requests for access, incidents, investigation, response on computers, receipts, reports, forwarding to a SIEM, updates and backups.

11.1 The Overview

The **Overview** (Figure 5.3) shows the state of the organization over the last 24 hours, 7 days or 30 days. Its tiles count the events, those blocked and those asked, the secrets touched in files and prompts, the open incidents, the approval requests that wait, the computers online and the seats in use. Below them: the activity of AI agents, allowed, asked and blocked; the AI agents with the most events; the **Risk leaderboard**, the people with the highest risk over the last 30 days, with their events and blocks of the same 30 days; **Secrets touched**, by kind of file and in prompts and uploads, which adds up to the tile **Secrets**; the hosts that AI agents connected to; the browser figures; the versions of IOArx Business in the fleet; and the newest events as they arrive. Drag across the bars of the activity to look at that period in **Investigate**. The bell at the top of the console counts the approval requests and open incidents that wait.

11.2 Approvals of Paused AI Agents

When a rule says Ask and the profile names an administrator to answer, the AI agent waits, paused with every process it started, and its request appears on **Approvals** at once, with a countdown (Figure 11.1).

1. Open **Approvals** (Figure 11.2). Under **AI agents waiting**, each card shows the AI agent and what it wants to do, the file or host, the computer, the person and the account, what the file holds, how many requests wait, and the time left. The link **Show the 3 programs behind it**, with the number of programs in the chain, shows the processes from the program that acted up to the AI agent.
2. Optionally, write **A note for the record**.
3. To keep the answer as a rule, choose in the list **Remember for this file** or **Remember for its folder**, or for a connection **Remember for this host** or **Remember for every destination**, and choose where the rule goes (Table 11.1). Keep **Only this time** to answer this request alone.
4. Choose **Allow** or **Block**.

The answer reaches the computer at once. When the time runs out without an answer, the computer stops the AI agent, and the request shows **No answer in time**. An AI agent waits as long as its profile says, from 10 seconds to one hour. Keeping an answer as a rule needs the permission **Change access profiles**. The view **Answered** lists every request with its answer, who answered, and the

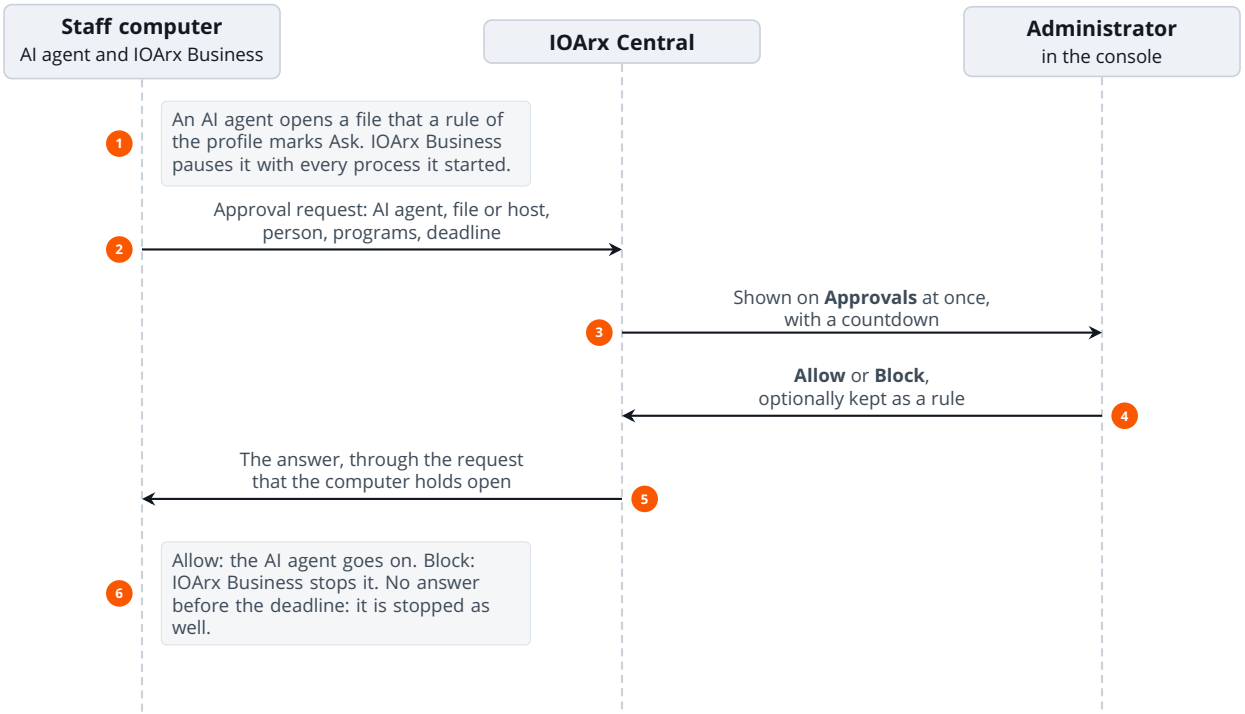


Figure 11.1: An AI agent waits for an administrator

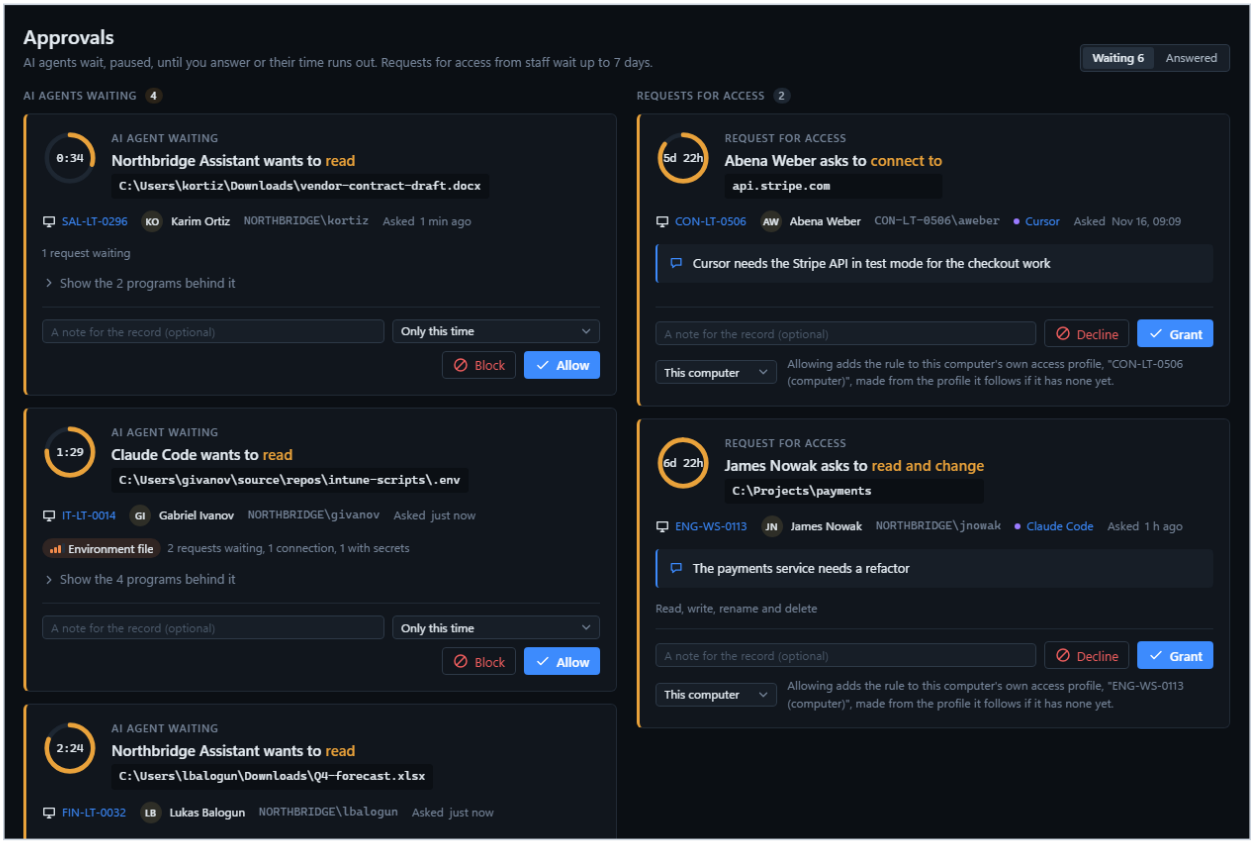


Figure 11.2: Approvals: AI agents that wait for an answer, and requests for access from staff

note.

Table 11.1: Where a kept answer, or a granted request for access, goes

Choice	Where the rule goes
This computer	The own profile of the computer, named `<computer name> (computer)`. If the computer has none yet, Central makes it as a copy of the profile that the computer follows now, and sets it on the computer. The rule reaches only that computer.
This person	The own profile of the person assigned to the computer, named `<person> (personal)`, made as a copy of the person's current profile if they have none yet. The computer needs an assigned person.
The profile of the computer	The profile that the computer follows, for every computer that follows it.

> **Important.** A profile made for one computer or one person is a copy. Later changes of the profile it was made from do not reach it. **Access profiles** marks such profiles with **One computer** or **Personal**; review them when you change the profile of their group.

11.3 Requests for Access

Staff ask ahead of time, in the IOArx Business app, to let an AI agent read or change a file or folder, or reach a host (Section 9.15). A request for access waits up to 7 days under **Requests for access** on **Approvals**.

1. Open **Approvals**. Each card under **Requests for access** shows the person, the computer, the AI agent, the file, folder or host, the access asked for, and the reason the person gave.
2. Choose where the rule goes: **This computer**, the default, **This person** or **The profile of the computer** (Table 11.1).
3. Choose **Grant** or **Decline**.

Grant adds a rule: for a file or folder, a rule for the path that allows reading, or for **Read and change** reading, writing, renaming and deleting; for a host, a network rule. **Decline** changes no profile. The person sees the answer in the app.

11.4 Incidents

Central opens an incident for every event of high or critical severity (Table 11.2), such as an AI agent that read an SSH key, a secret sent to an AI service anyway, or a sign of tampering on a computer. Later events of the same AI agent on the same computer, of the same AI service in its browsers, or of the same sign join the open incident when they come within 30 minutes of its events, whatever their own severity.

1. Open **Incidents**. Filter by status (**Needs work**, **Open**, **Investigating**, **Resolved**, **False positive**, **All**), by severity and by assignee.
2. Open an incident. Its timeline lists its events, notes and changes, newest first.

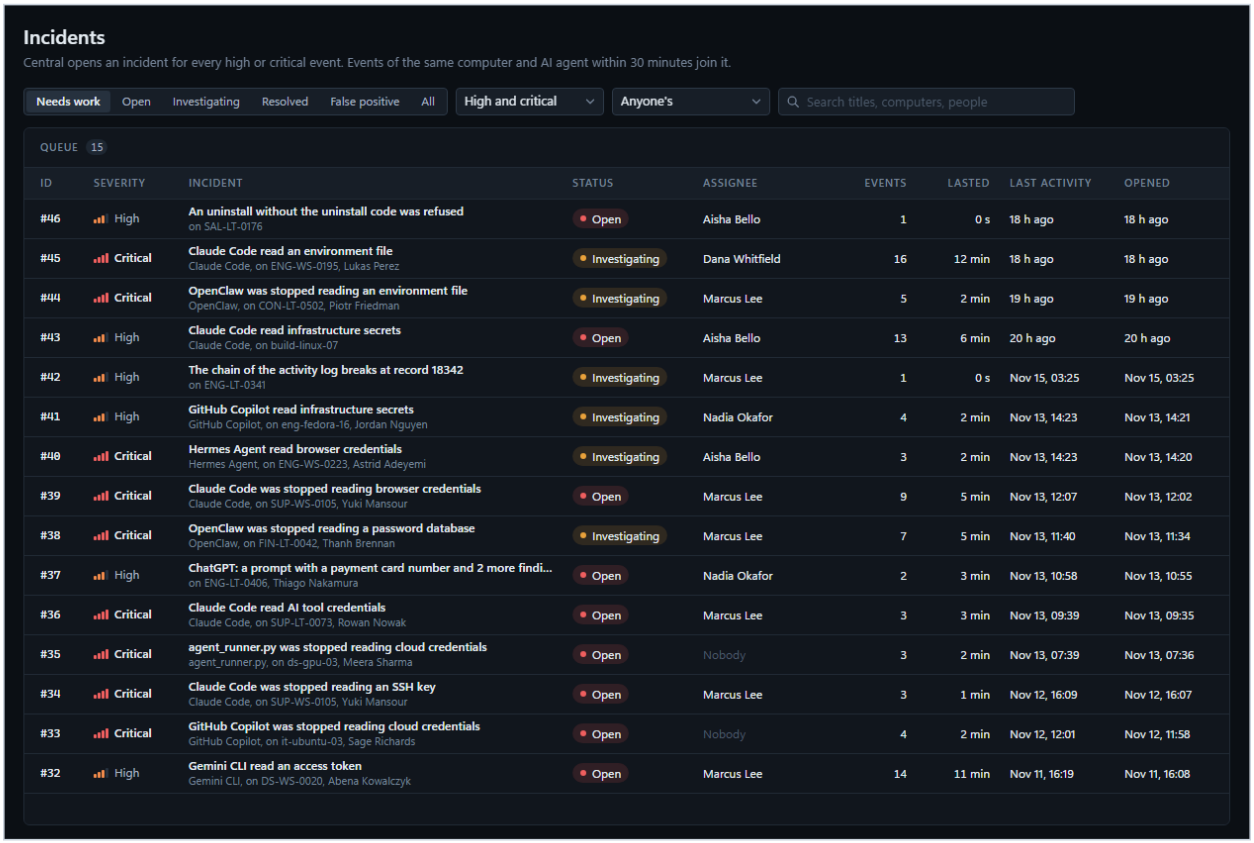


Figure 11.3: The queue of incidents

3. Under **Work on it**, set the **Status**, take the incident with **Take it** or choose the **Assignee**, and set the **Severity**.
4. Under **Add a note**, write what you found and did, and choose **Add note**.
5. Under **Respond on the computer**, isolate the computer, stop the AI agent, or lock a file or folder (Section 11.6).
6. Choose **Resolve** when the incident is closed.

Table 11.2: How Central sets the severity of an event

Event	Severity
File access	What the file holds and what the content scan found set the severity, up to critical. A blocked access is at least medium. An access that an AI agent was allowed, or that the person at the computer allowed, is at least low.
Connection	Info when a rule or an administrator allowed it, low when the person at the computer allowed it, medium when it was blocked.
Browser	The findings set the severity, at least low. A prompt or a file sent anyway counts one step higher, and at least medium, since what was found left the organization.
Computer	High for a break in the log chain, a start without a clean stop, a jump of the clock and an uninstall without the code. Medium for the other signs of Table 12.1.

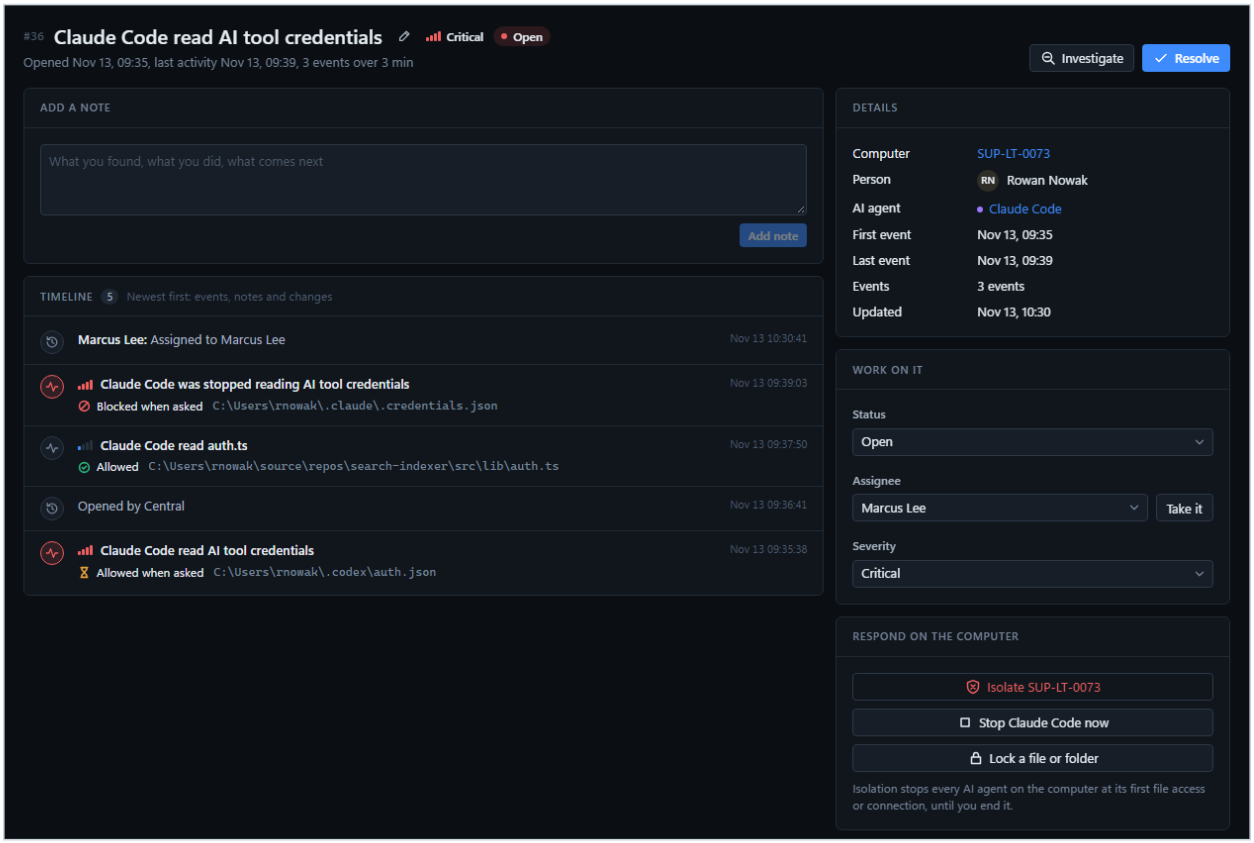


Figure 11.4: An incident, with its timeline and the response on the computer

11.5 Investigation

Investigate holds every event of every computer: file accesses and connections of AI agents, what IOArx for Browsers stopped, behavior detections, the use of AI services, and the events of the services themselves.

- Choose the period, **1 hour**, **24 hours**, **7 days** or **30 days**, or drag across the histogram to choose another one.
- Add filters with **Filter**: the outcome, the severity, the kind, who decided, and the AI agent. Type text into the search field to search the target, program, AI agent, account or computer, and press Enter.
- Open an event. Its drawer shows the **Summary**, the **Process chain** from the program that acted up to the AI agent, the **Rule** that decided, and the **Record** as the computer wrote it, with its hash and whether it continues the chain of the log of the computer. Pivot from it to **This computer**, **This AI agent**, **This person** or the **Graph**.
- Choose **Export** and **Events as CSV** or **Events as JSON** to save the events that the filters select, up to 100,000 events in one file. Export needs the permission **Export events**, and every export goes into the audit log.

Graph shows who, on which computer, with which AI agent, touched what: people, computers, AI agents, kinds of secrets and hosts as nodes, with red links where events were blocked. Each type of node gets a share of the nodes shown, from 60 to 250 in all; the legend lists the types present, and

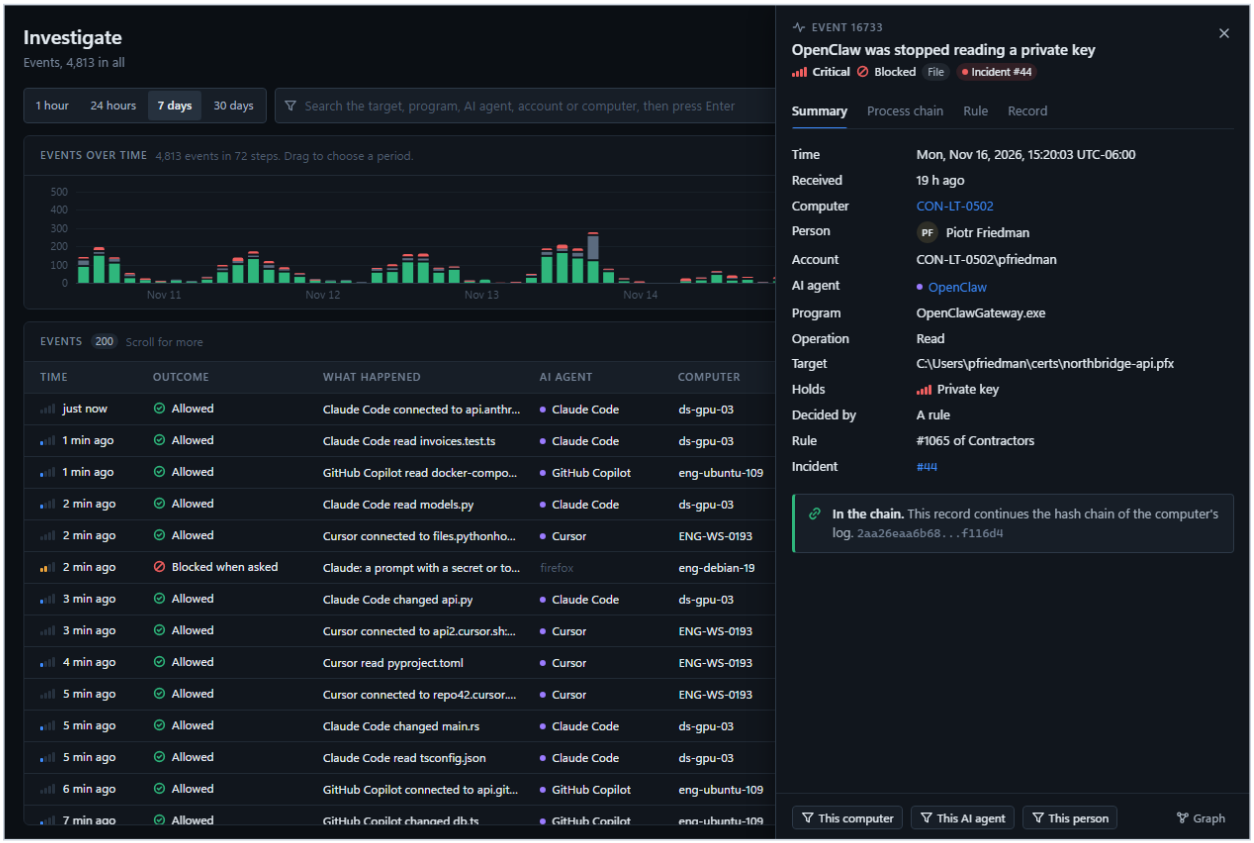


Figure 11.5: Investigate, with the details of one event

hides or shows a type. Opening a node shows its links in a panel, and the graph lays itself out beside it. **Live feed** lists the events as the computers report them. **AI inventory** (Figure 11.6) lists every AI agent seen in the organization: on how many computers and for how many people, how it was recognized, when it was first and last seen, and how often it was stopped.

11.6 Responding on a Computer

The page of a computer, the menu of its row under **Computers**, and the page of an incident offer the response on that computer.

Table 11.3: Actions on a computer

Action	What it does
Isolate	Every AI agent on the computer is stopped at its first file access or connection, whatever the profile allows: the computer blocks AI agents on every drive and on the network. People keep working. Confirm by typing the name of the computer. **End isolation** undoes it.
Lock a file or folder	No program of a signed-in person opens the file or folder until you unlock it. Type the path, with * for one folder level, and the reason under **Why**. The tab **Locks** shows each lock as **Waiting**, **Locked** or **Refused** with the reason; **Unlock** restores the previous access.

Action	What it does
Stop an AI agent	Every process of the AI agent, with every program it started, ends at once. Work it had not saved is lost.
Send a message	A notification, with a title of up to 80 characters and a message of up to 400, for the people signed in at the computer.
Refresh the policy	The computer calls in for its policy now.
Look for AI agents now	The computer looks for running AI agents and reports them.
Request a receipt of the log	The computer sends a signed receipt of its activity log (Section 11.7).
Restart the service	IOArx Business restarts on the computer. Protection pauses for a few seconds.
Retire	Frees the seat; IOArx Business removes itself from the computer (Section 13.1).

Isolation and locks reach the computer with its next heartbeat; the other commands reach it within seconds when it is online. The tab **Commands** of the computer lists the newest 50 commands with their status, **Queued**, **Sent**, **Done** or **Failed**, and their result. Isolation, locks, stopping an AI agent, messages, refreshing the policy, looking for AI agents and receipts need the permission **Lock files and folders, isolate computers and stop AI agents**; restarting the service and retiring need **Manage computers**.

11.7 Receipts of the Activity Log

Each computer writes every decision to its activity log, each record tied to the one before by its SHA-256 hash, and Central checks that every batch continues the chain it already holds. A receipt is a summary of the log as it is on the computer, with the number of records and the hash at its head, signed with the key of the computer. Central compares it with the records it holds.

1. Open the computer and the tab **Receipts**, and choose **Request a receipt**.
2. When the receipt arrives, read the columns **Check**, which shows **Intact**, **Altered**, **Records missing** or **Checking**, and **Signature**, which shows **Verified** or **Not verified**.

11.8 Reports and Exports

Reports makes a summary of a period, **7 days**, **30 days**, **90 days** or **This month**, for management, auditors and the data protection officer: the activity, the incidents and how they ended, the approval requests and their answers, the computers without protection, the AI inventory, the browser figures, the changes that administrators made, and the access profiles in force with their versions. **Print** prints it, or saves it as PDF from the print dialog. Events leave the console as CSV or JSON from **Investigate** (Section 11.5).

11.9 Forwarding to a SIEM

Central forwards events to a syslog server, to a webhook, or to both, from the moment you turn forwarding on.

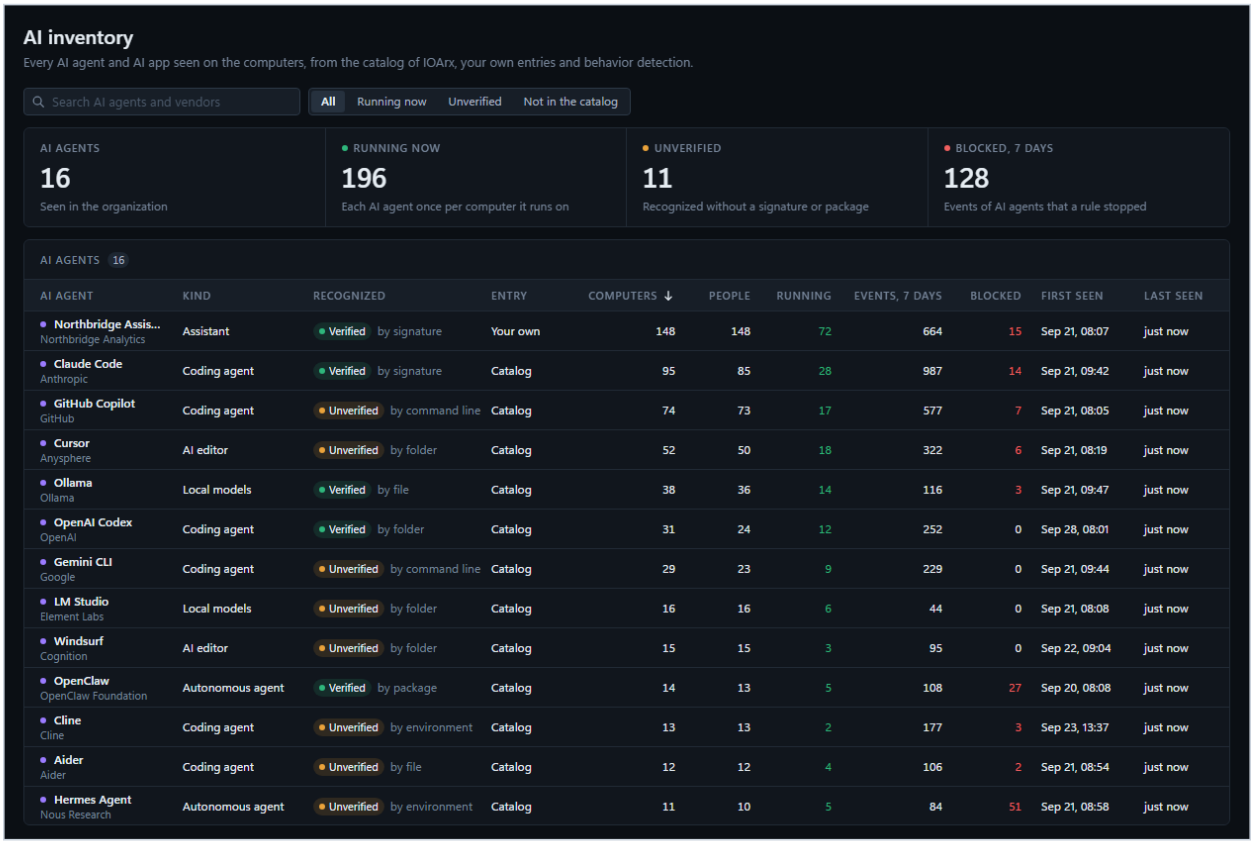


Figure 11.6: The AI inventory: every AI agent seen in the organization, and how it was recognized

1. Open **Settings** › **SIEM**.
2. For syslog, turn on **Syslog** and fill in the **Host** and the **Port**, 514 by default. Choose the **Protocol**, **UDP** or **TCP**, the **Format**, **RFC 5424 with JSON** or **CEF**, and under **Send** the lowest severity to forward: **Every event**, **Low and up**, **Medium and up**, **High and up**, the default, or **Critical only**.
3. For a webhook, turn on **Webhook**, type the **Address**, a **Secret** that signs each request, and the lowest severity under **Send**.
4. Choose **Save**, then **Send a test event**. The page shows for each destination whether the test event went out, or the error.

Syslog

Each event is one syslog message of RFC 5424, with facility 10 (security), the app name `ioarx-central`, and the kind of the event as message id: `file`, `connect`, `browser`, `detection`, `usage` or `system`. The severity of the message follows the event: critical 2, high 3, medium 4, low 5, info 6. The message holds the event as JSON, or as CEF. Over TCP, messages are framed by octet counting (RFC 6587); over UDP, each event is one datagram of at most 8,192 bytes. Syslog messages travel unencrypted: send them only within a network you trust, or use the webhook over HTTPS.

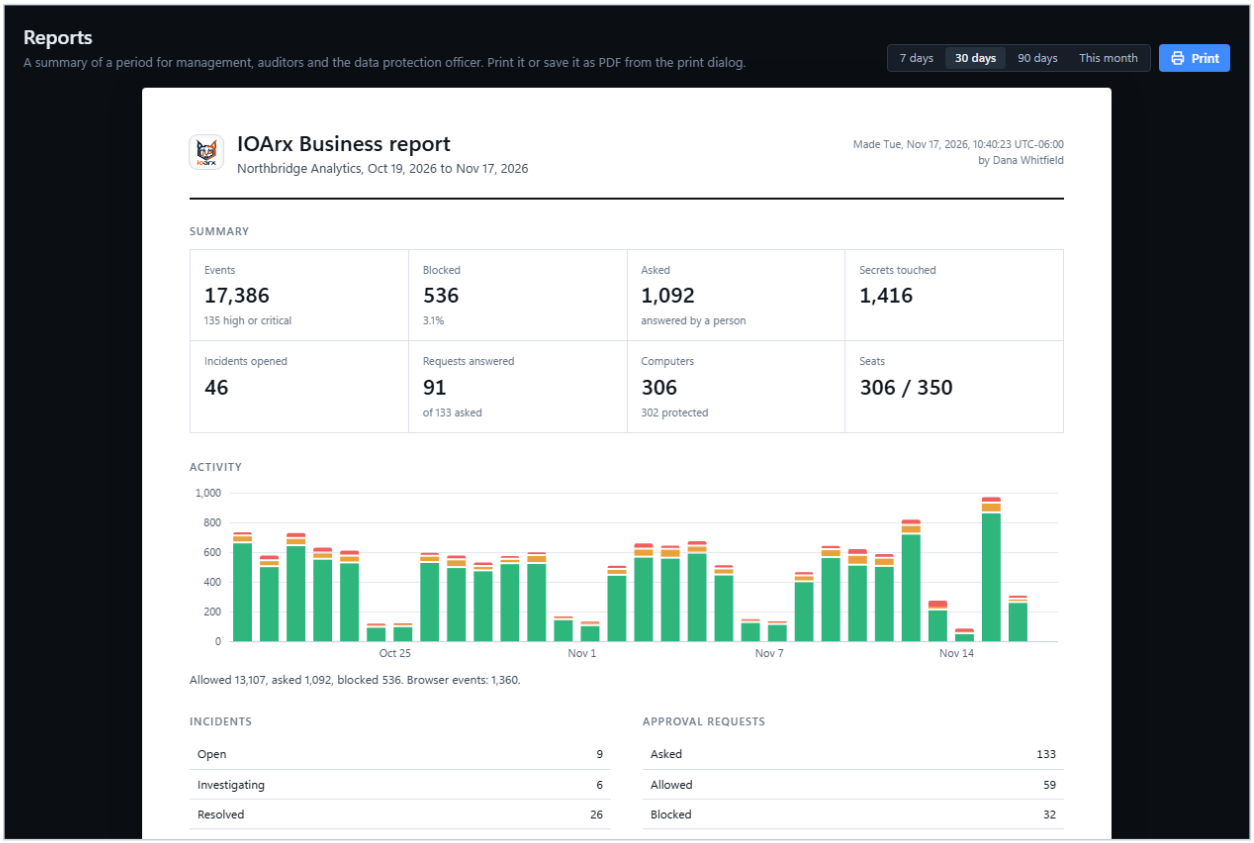


Figure 11.7: A report of 30 days

CEF

The header is `CEF:0|IOArx|IOArx Central Monitoring|<version>|<kind.operation>|<title>|<severity>`, with the severity 10 for critical, 8 for high, 5 for medium, 3 for low and 1 for info.

Table 11.4: Fields of a CEF message

Field	Value
`rt`	The time of the event, in milliseconds since 1970.
`externalId`	The id of the event in Central.
`dvchost`	The name of the computer.
`duser`	The account on the computer.
`suser`	The person, or a pseudonym when pseudonyms are on.
`act`	The decision: `allow` or `deny`.
`outcome`	Who decided: `rule`, `employee`, `administrator`, `timeout` or `overflow`.
`fname`	The target: a path, a host and port, an AI service, or what happened.
`cs1` (`cs1Label=agent`)	The AI agent.
`cs2` (`cs2Label=sensitive`)	The kind of secret that the file holds.

Field	Value
`sproc`	The program.
`cs3` (`cs3Label=incident`)	The incident the event belongs to.
`cn1` (`cn1Label=rule`)	The id of the rule that decided.
`msg`	The title of the event, such as `Claude Code read an SSH key`.

Webhook

Central sends an HTTPS POST with a JSON body of the form `{"source": "IOArx Central Monitoring", "organization": "...", "events": [...]}` and the header `x-ioarx-signature: sha256=<hex>`, where `<hex>` is the HMAC-SHA256 of the raw body with the secret, in lower-case hexadecimal. A receiver checks the signature before it trusts the body, for example in Python:

Python

```
import hashlib, hmac

def signature_holds(body: bytes, header: str, secret: str) -> bool:
    expected = "sha256=" + hmac.new(secret.encode(), body, hashlib.sha256).hexdigest()
    return hmac.compare_digest(expected, header)
```

Each event carries the fields that **Investigate** shows: `id`, `time_ms`, `received_ms`, `device`, `person`, `account`, `kind`, `operation`, `verdict`, `decided_by`, `agent`, `program`, `target`, `sensitive`, `findings`, `severity`, `rule`, `incident_id`, `approval_id` and `title`.

Central forwards up to 200 events at a time. Each destination keeps its own position in the events and moves on only once a batch went out, so nothing is lost while the SIEM cannot be reached; Central tries again with growing pauses of up to 5 minutes. A destination that you turn on starts with the events that arrive after it, not with the history. With pseudonyms on, the SIEM receives pseudonyms, never names. The webhook secret is sealed in the database and never written to a log.

11.10 Updates

Central reads the update feed `https://ioarx.com/updates/business/latest.json` twice a day, downloads the packages of IOArx Business for each system and the newest installer of IOArx Central Monitoring, and checks each against its signature with the update key of IOArx. Each computer downloads its package from Central, checks its size, its SHA-256 hash and the signature again with the key built into it, and installs it without a window. A Central that was taken over still cannot make a computer run a program that IOArx did not sign.

Table 11.5: Which version the computers run

Choice under Updates	What happens
The newest package	Each computer installs the newest package for its system when it calls in. This is the default.
A version I choose	Computers that run an older version install the version you choose. Computers that run a newer version keep it: a computer never installs an older version.

Choice under Updates	What happens
Hold updates	Computers stay on the version they run, and new computers run the version of their installer. Central does not look for new versions by itself.

The page **Updates** (Figure 11.9) also shows the versions in the fleet and every package that Central holds, with its file, size, SHA-256 hash, where it came from, and whether its signature is **Verified**. **Check ioarx.com** looks for a new version at once. The list also holds the newest installer of IOArx Central Monitoring, as **IOArx Central, Windows 64-bit**, so that the page shows when a new version of Central is out. Central does not install it itself: install it with the console on the Central computer (Section 11.10.2).

11.10.1 Networks without internet access

1. On a computer with internet access, download the package and its signature file from `https://ioarx.com/updates/business/`, for example `IOArx-Business_1.0.0_x64-setup.exe` and `IOArx-Business_1.0.0_x64-setup.exe.sig`. Keep the file names as they are.
2. Copy both files into one folder on a computer with the console.
3. Under **Updates**, choose **Import a package** and choose the package. The console reads the `.sig` file next to it, and Central checks the signature of IOArx before it keeps the package.

Repeat this for each system: the x64 and x86 installers, the deb package, the rpm package and the installer of IOArx Central Monitoring.

11.10.2 Update Central and the consoles

IOArx Central Monitoring updates through its console. Under **Updates**, the panel **Central and this console** shows the versions of IOArx Central and of the console in use. **Check for a new console** asks `ioarx.com`, from the computer on which the console runs, for a newer version of IOArx Central Monitoring. The button **Install**, with the new version number, downloads it, checks its signature and runs its installer.

- On the Central computer, the panel says **The console updates itself and the Central service on this computer together, from ioarx.com.** The update installs the console and the IOArx Central service together, and keeps the database, `central.json` and the role of the computer. The installer stops the service, replaces the programs, sets the service up again and starts it.
- On the computer of an administrator with the console alone, the panel says **This console updates itself from ioarx.com. IOArx Central updates with the console on the Central computer.** The update changes that console only.

When administrators work from consoles on their own computers, update in this order:

1. Make a backup of Central (Section 11.11).
2. On the Central computer, open IOArx Central Monitoring, sign in, and under **Updates** choose **Check for a new console**, then **Install** with the new version number. Or run the new installer of IOArx Central Monitoring there as an administrator: it keeps the role of the computer, also with `/S`.
3. On the computer of each administrator, update the console in the same way, or run the new installer there: it keeps the console alone, also with `/S`.

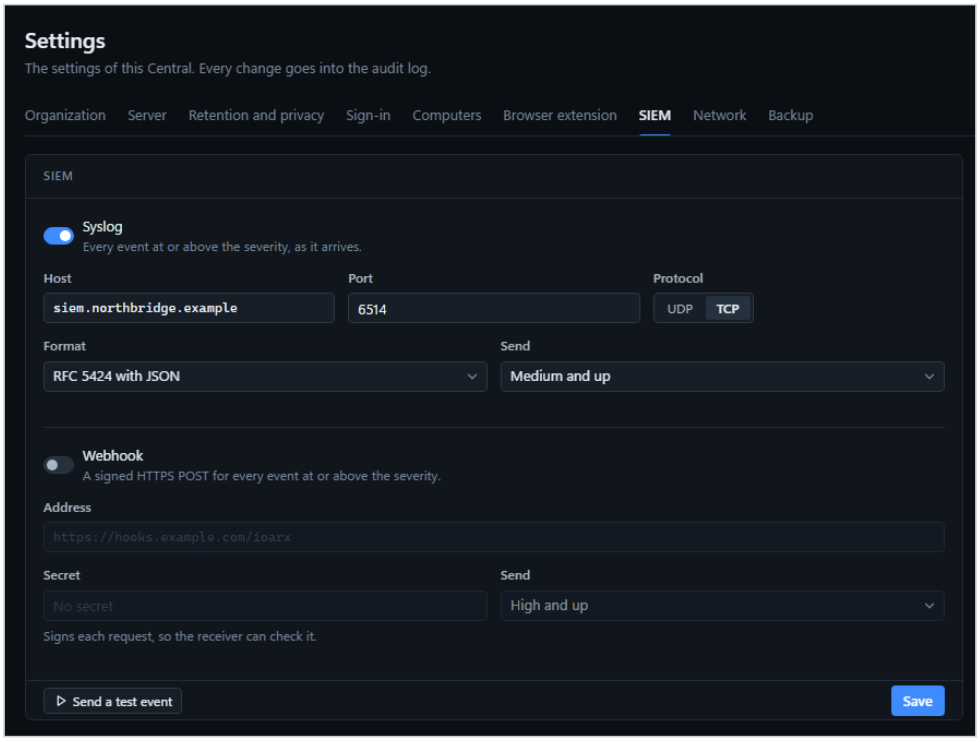


Figure 11.8: Forwarding to syslog over TCP

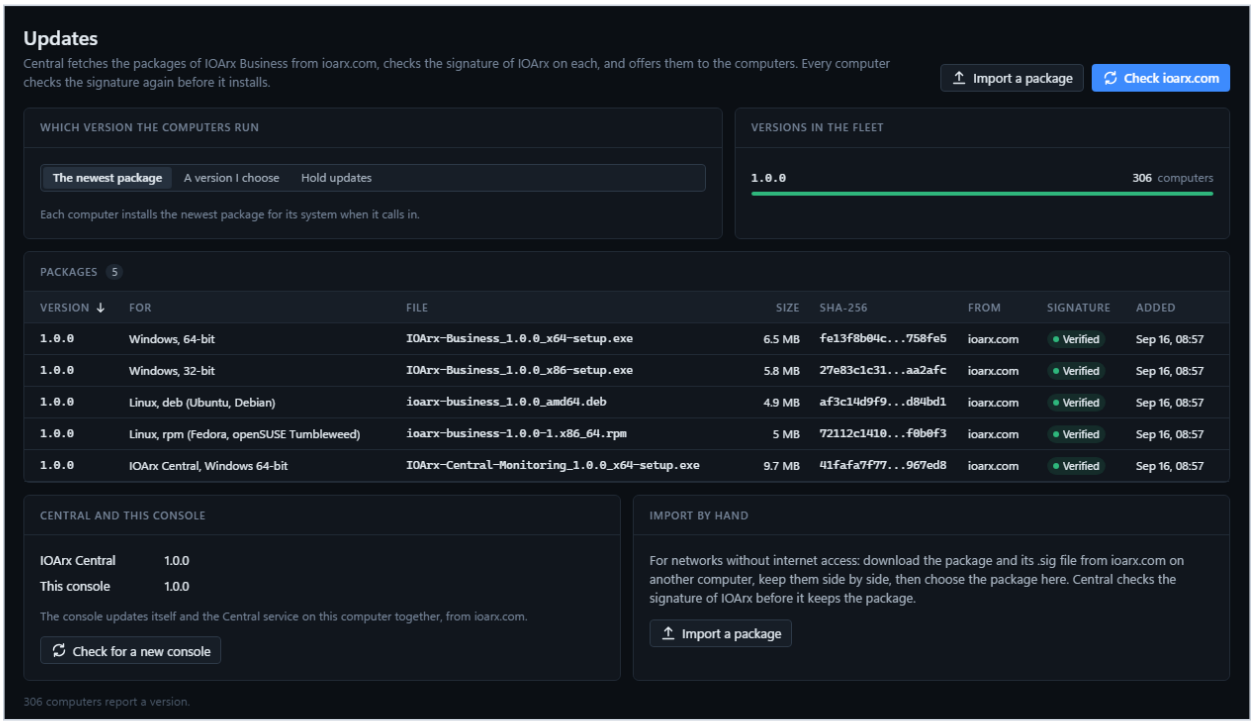


Figure 11.9: Updates: the rollout, the versions in the fleet and the packages that Central holds

> **Important.** Updates, and the installer run again on a computer that has IOArx Central Monitoring, also silently, keep the role of the computer: the IOArx Central service where it runs, the console alone where it does not. To turn a computer with the console alone into the Central computer, uninstall the console first, then install IOArx Central Monitoring and answer **Yes**.

11.11 Backups and Restore

1. Open **Settings** › **Backup** and choose **Make a backup now**. Central writes a consistent copy of its database while it keeps running, to `C:\ProgramData\IOArx Central\backups\central-<time>.db`, and keeps the newest 10 backups there.
2. Copy the backups to your backup storage, together with the copy of the folders `tls` and `keys` (Section 4.8).

Make a backup before every update of Central and on a regular schedule. Backups need the permission **Change the settings of Central** and the whole organization as scope.

11.11.1 Restore Central

Restore Central on a computer that the staff computers reach at the same address: the same computer, or another one to which you move the DNS name of Central.

1. Install IOArx Central Monitoring on the computer as the Central computer (Section 4.2).
2. Stop the service:

   Command Prompt, as an administrator

   ```
   sc stop IOArxCentral
   ```

3. Put the folders `tls` and `keys` from your copy into `C:\ProgramData\IOArx Central`, in place of the ones there.
4. Delete `central.db-wal` and `central.db-shm`, and copy the backup in place of `central.db`.
5. Start the service:

   Command Prompt, as an administrator

   ```
   sc start IOArxCentral
   ```

6. On a computer other than the one before, open the console, sign in and activate the license key (Section 6.2). Release the activation on the earlier computer first if it still runs (Section 6.7). If it no longer runs, `ioarx.com` answers that the key is active in another IOArx Central Monitoring; ask IOArx through `https://ioarx.com/contact` to release it.

The computers then find Central with the certificate they know. Without the folder `tls`, Central has a new certificate, which the computers do not trust: on each computer, remove IOArx Business with its uninstall code and install it again with a new enrollment token, which makes it join as a new computer (Section 13.3). Each new record takes a seat of its own, so retire the earlier records afterwards. Without the folder `keys`, two-factor sign-in must be set up again, the webhook secret and

the proxy must be entered again under **Settings**, and Central can no longer show the uninstall codes of the computers; retiring a computer still removes IOArx Business from it.

> **Note.** Central lacks the events that computers sent after the backup was made. For each computer that sent events in that time, Central reports a break in the chain of its activity log at the first record it receives after the restore, and opens an incident (Table 12.1). A break at a record from between the backup and the restore comes from the restore.

11.11.2 When every Owner has lost access

On the Central computer, as an administrator of that computer:

Command Prompt, as an administrator, on the Central computer

```
"C:\Program Files\IOArx Central Monitoring\ioarx-central-server.exe" reset-owner
    ↪ --username dana.whitfield
```

The command prints a temporary password, which the Owner must change at the next sign-in. It also lifts a lock of the account, ends its sessions and turns its two-factor sign-in off; turn two-factor sign-in on again after signing in. The audit log records the reset.

CHAPTER 12

Security Model

This chapter describes how IOArx Business protects the staff computers, itself and the data it handles, for the security review of an organization. Chapter 2 describes the parts and how they trust each other; this chapter adds what each part does against tampering and misuse.

12.1 Protection on the Staff Computers

- Protection runs as a service from the start of the computer, before anyone signs in. On Windows, the service `IOArxBusiness` runs `ioarx-endpoint.exe` as LocalSystem, starts automatically and restarts after a failure. On Linux, the systemd services `ioarx-monitor` and `ioarx-business` run as root and restart after a failure.
- The IOArx Business app of each person is a window onto the service. Closing the app, or ending it, changes nothing about protection.
- The app has no control that changes a rule, an AI agent or a setting. Staff ask for access in the app, and administrators decide in the console (Section 11.3).
- Every file access and connection of an AI agent goes through the rules of the access profile. Ask pauses the AI agent, with every process it started, until the answer comes; Block stops it.
- The operating system enforces locks. A locked file or folder is open only to SYSTEM and Administrators on Windows, or belongs to root with mode 0700 or 0600 on Linux, so that no program of a signed-in person opens it. Unlocking restores the access it had before.

12.2 Tamper Protection

The option **Tamper protection**, under **Computers** in the access profile (Section 7.13), is on by default. With tamper protection on:

- The access list of the service `IOArxBusiness` lets only SYSTEM stop, pause, reconfigure or delete it. Administrators of the computer, like every signed-in user, can only query it.
- The uninstaller on Windows and the package scripts on Linux remove IOArx Business only with the uninstall code of the computer (Section 12.4), or after Central retired the computer.
- An attempt to uninstall without the code is refused and reported to Central, where it opens an incident.
- An enrollment token left on an enrolled computer is ignored, so that nobody can move the computer to another Central (Section 13.3).

With tamper protection off, the service has the access list that Windows gives every new service, which lets administrators of the computer stop it, and IOArx Business can be removed without a code. A computer that never enrolled can always be removed without a code. On Linux, root keeps control of the systemd services in either case; a computer whose service stops shows as offline in

Central (Section 14.4).

The data folder of the service, `C:\ProgramData\IOArx Business` on Windows and `/var/lib/ioarx-business` on Linux, is open only to SYSTEM and the Administrators group, or to root. It holds the identity and the key of the computer, the last policy, the activity log and the events that wait to be sent.

> **Important.** Tamper protection keeps protection out of the hands of the people who use a computer. An administrator of the computer, or root on Linux, can open the data folder, which holds the key of the computer. Give staff standard user accounts, and keep administrator rights on staff computers with the IT department.

12.3 Signs of Tampering

Each computer reports what happens to IOArx Business itself, and Central adds what it notices. A sign of high severity opens an incident (Section 11.4), and the page of the computer shows the newest one under **Sign of tampering** for 7 days.

Table 12.1: Signs of tampering that Central reports

Sign, as the console shows it	Severity	What it means
The chain of the activity log breaks at record <n>	High	A record does not continue the chain of hashes: records on the computer were changed, removed or cut off, or Central never received the records before it. The page of the computer shows **The log chain is broken**.
IOArx Business started after it was ended from outside or the computer lost power	High	The service started without the mark that a clean stop leaves.
The clock jumped <time> forward, or **back**	High	The clock of the computer was set forward or back by 5 minutes or more at once. Every 30 seconds, the service compares the clock with the time since the start of the computer, sleep included, so waking from sleep is no jump.
An uninstall without the uninstall code was refused	High	Someone tried to remove IOArx Business without the code. The details of the event name the account.
IOArx Personal is installed on this computer as well	Medium	Both editions of IOArx run on the computer. Uninstall IOArx Personal: IOArx Business takes its place.
<path> could not be locked	Medium	A lock did not take effect. The tab **Locks** of the computer gives the reason.
<path> could not be unlocked	Medium	A lock that Central removed is still in place. The computer tries again with every policy.
IOArx Business <version> could not be installed	Medium	An update failed on the computer. The details of the event give the reason.
<computer> has not called in for 7 days	Medium	Central reports, once, a computer that stopped calling in.

Sign, as the console shows it	Severity	What it means
Enrolled with the identity of <computer>	Medium	A computer enrolled with the machine identifier of a record that Central already holds (Section 13.3).

12.4 Uninstall Codes

Every computer has an uninstall code of its own: ten characters in two groups, such as `K7Q2M-XW4PA`. At enrollment, Central gives the computer a secret of 32 random bytes and keeps it sealed in its database. The code is made from that secret, so the computer checks a code itself, without a connection to Central. Upper and lower case, spaces and hyphens make no difference when the code is typed.

Administrators with the permission **Manage computers** find the code on the page of the computer, in the panel **Uninstall code**, with **Show** and **Copy**. Give the code only to the person who removes IOArx Business from that computer; it works on no other computer. Giving the code also releases the identity of the computer: with a new enrollment token, it then joins as a new computer (Section 13.3). Without the folder `keys` of Central, Central can no longer show the codes (Section 11.11.1).

12.5 Limits on Connections and Requests

Section 2.4 describes how computers and consoles trust Central by its pinned certificate, and how Central knows each computer by its signed requests. Central also limits what one computer or one network address can ask of it, so that a faulty or hostile client cannot crowd out the others. A computer that reaches a limit waits and sends again.

Table 12.2: Limits that Central applies

What	Limit
Requests of one computer	300 a minute
Data that one computer sends	64 MB a minute
Requests of one computer that wait for an answer	2 at once
Signed requests of one computer	5,000 within 10 minutes
Approval requests of one computer that wait for an answer	100
Connections from one network address	1,000 at once; from 16 to 20,000 with `connections_per_address` in `central.json`
Connections in all	20,000 at once
Refused enrollment tokens from one network address	20 within 10 minutes
Sign-in attempts from one network address	30 within 10 minutes
Wrong passwords in a row for one administrator	5, then the account is locked for 15 minutes

12.6 Administrators of Central

- Passwords have at least 12 characters, and Central keeps them as Argon2id hashes.
- Two-factor sign-in uses an authenticator app (TOTP, RFC 6238), and the organization can require it of every administrator (Section 5.4).
- Sessions end after a time without use, 30 minutes by default, and after 12 hours in all (Section 5.8).
- Roles grant permissions, and scopes limit an administrator to groups of computers (Section 8.5 and Appendix D). At least one active administrator always holds the role Owner.
- The audit log records every change that an administrator makes, chained by hashes like the activity log of a computer. The page **Audit log** (Figure 12.1) shows **The chain holds** as long as no entry was changed or removed.
- The password of an Owner who cannot sign in is reset only on the Central computer, by an administrator of that computer (Section 11.11.2).

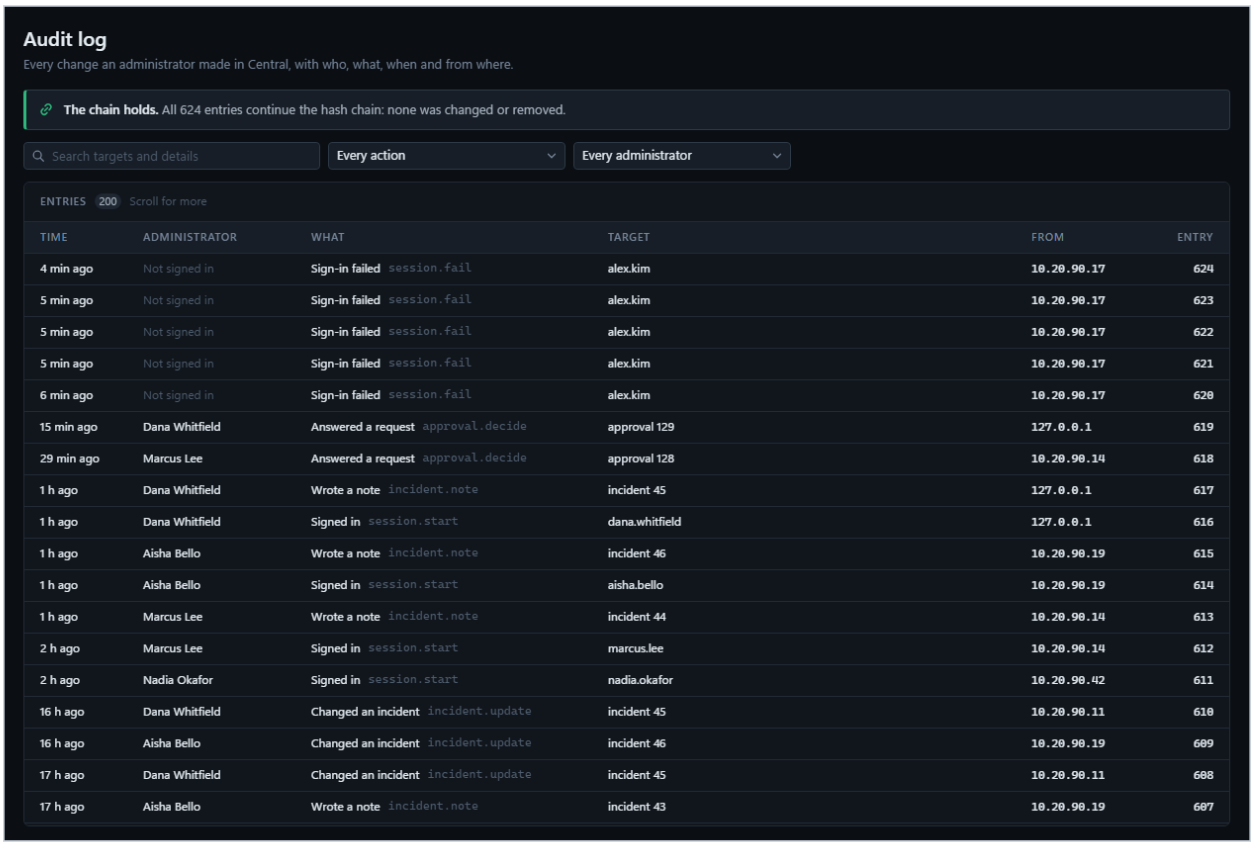


Figure 12.1: The audit log, with the state of its hash chain

12.7 Central Itself

- The service `IOArxCentral` runs under its own virtual account, `NT SERVICE\IOArxCentral`, not as LocalSystem.
- Its data folder is open only to SYSTEM, the Administrators group and that account, without

inherited entries (Section 4.5).

- Central takes its first setup only from the computer it runs on, so that nobody else on the network can make themselves its Owner.
- Central checks every request of a console for the permission it needs and for the scope of the administrator.
- The key `keys\vault.key` seals the secrets that Central keeps in its database: the keys of two-factor sign-in, the secrets behind uninstall codes, the webhook secret and the proxy password.
- The log of the service, `logs\central.log`, holds no passwords, tokens, keys or contents of events.

12.8 Updates

IOArx signs every package of IOArx Business with minisign (Ed25519), using the update key of IOArx, key id `1C60F3ED26F349E8`. Central checks the signature when it downloads or imports a package, and every computer checks it again, with the key built into IOArx Business, before it installs. A Central that was taken over still cannot make a computer run a program that IOArx did not sign. The console of IOArx Central Monitoring installs only new versions signed with the same key. Every Windows program and installer of IOArx Business and IOArx Central Monitoring also carries an Authenticode signature, made through Azure Artifact Signing, with an RFC 3161 time stamp.

CHAPTER 13

Retiring Computers and Uninstalling

A computer leaves the organization in one of two ways: an administrator retires it in the console, and IOArx Business removes itself; or someone with its uninstall code removes IOArx Business on the computer. Only retiring frees the seat of the computer.

13.1 Retire a Computer

1. Open **Computers** and the computer.
2. Open the menu **More actions**, the button with three dots at the top right of the page, and choose **Retire**. The menu of the row of the computer under **Computers** offers the same.
3. Type the name of the computer, and choose **Retire the computer**.

Retiring needs the permission **Manage computers**. Then:

- The seat is free at once. The page of the computer shows **Retired. The computer uninstalls IOArx Business at its next call.**
- At its next call, the computer ends protection, removes its folder locks and the browser policies it wrote, and removes IOArx Business: on Windows with its uninstaller, on Linux with `dpkg -r` or `rpm -e`.
- The computer reports the command as done, and Central marks it as retired. A computer that does not call in within 7 days is marked as retired then, and removes IOArx Business whenever it calls in later.
- The events of the computer stay in Central.
- The data folder of IOArx Business stays on the computer, with the mark of its retirement. A new installation with an enrollment token makes the computer join as a new computer (Section 13.3).

13.2 Uninstall IOArx Business on a Computer

Removing IOArx Business on the computer needs its uninstall code (Section 12.4), unless Central retired the computer, its profile turns tamper protection off, or it never enrolled. Uninstalling does not free the seat: retire the computer in the console as well.

13.2.1 Windows

The uninstaller takes the code on its command line. In a Command Prompt that runs as an administrator:

Command Prompt, as an administrator

```
"C:\Program Files\IOArx Business\uninstall.exe" /CODE=<uninstall code>
```

The uninstaller opens its window. Its option to delete the application data deletes the data folder `C:\ProgramData\IOArx Business` as well. To remove IOArx Business without a window, add `/S`; the data folder then stays:

Command Prompt, as an administrator

```
"C:\Program Files\IOArx Business\uninstall.exe" /S /CODE=<uninstall code>
```

The uninstaller returns at once and finishes from a copy in the temporary folder of Windows. Check the removal a minute later:

Command Prompt

```
sc query IOArxBusiness
```

After the removal, `sc query` answers that the service does not exist (error 1060). While the service is still there, the uninstaller refused: without the right code, it shows the message below and quits, or quits without a message under `/S`, and Central records the attempt (Table 12.1).

> *IOArx Business is managed by your organization. To remove it, ask your administrator to retire this computer in IOArx Central Monitoring, or run the uninstaller with the uninstall code of this computer: uninstall.exe /CODE=XXXXX-XXXXX*

13.2.2 Linux

The package scripts read the code from the variable `IOARX_UNINSTALL_CODE`:

Ubuntu and Debian

```
sudo IOARX_UNINSTALL_CODE=<uninstall code> apt remove ioarx-business
```

Fedora

```
sudo IOARX_UNINSTALL_CODE=<uninstall code> dnf remove ioarx-business
```

openSUSE Tumbleweed

```
sudo IOARX_UNINSTALL_CODE=<uninstall code> zypper remove ioarx-business
```

Without the right code, the removal stops with the message `IOArx Business is managed by your organization. Ask your administrator to retire this computer in IOArx Central Monitoring, or give its uninstall code in IOARX_UNINSTALL_CODE.` The removal stops both services, deletes the nftables table `inet ioarx`, and keeps the data folder `/var/lib/ioarx-business`. On Ubuntu and Debian, `apt purge` in place of `apt remove` deletes the data folder as well.

13.3 Install IOArx Business Again

A computer keeps its identity while it is enrolled: a token that an installer or `ioarx-endpoint enroll` leaves on it is ignored, so that nobody can move it to another Central. Two things release the identity: Central retires the computer, or someone gives its uninstall code, with `/CODE=` of the uninstaller, with `IOARX_UNINSTALL_CODE` on Linux, or with `ioarx-endpoint prepare-uninstall --code`.

Table 13.1: A new installation on a computer that ran IOArx Business before

The computer	What the new installation does
Was retired by Central	With a token: joins as a new computer, with a record and a seat of its own, and sends its whole activity log to the new record. Without a token: stays retired.
Its uninstall code was given	With a token: joins as a new computer, as above; the earlier record keeps its seat until you retire it. Without a token: takes up its earlier record again.
Was installed again from scratch, or lost its data folder	With a token: joins as a new computer, as above.

When a computer joins as a new computer with the machine identifier of an earlier record, Central adds the sign **Enrolled with the identity of <computer>** (Table 12.1), and the page of the computer names the earlier record of the same machine. Every enrollment makes a new record, so that an enrollment token in the wrong hands cannot take over a computer that Central knows.

To make an installed computer join another Central without installing it again, give its uninstall code, then the token of the other Central:

Command Prompt, as an administrator

```
"C:\Program Files\IOArx Business\ioarx-endpoint.exe" prepare-uninstall --code <uninstall
    ↪ code>
"C:\Program Files\IOArx Business\ioarx-endpoint.exe" enroll --token <enrollment token>
```

Linux

```
sudo ioarx-endpoint prepare-uninstall --code <uninstall code>
sudo ioarx-endpoint enroll --token <enrollment token>
```

13.4 Move Central to Another Computer

The computers find Central at the addresses of their newest policy and trust it only by its certificate. Move Central with its certificate. To give Central only a new name or address on the same computer, follow Section 3.5.

1. If the new computer will have another name or address than Central has now, add it under **Settings** › **Server** on the old Central, and wait until the computers in use have applied their newest policy (Section 3.5).
2. Install IOArx Central Monitoring on the new computer as the Central computer (Section 4.2); if

the console alone is installed there, uninstall it first. Then stop the service:

Command Prompt, as an administrator, on the new computer

```
sc stop IOArxCentral
```

3. On the old Central, open **License** and release the activation (Section 6.7). Stop its service at once with `sc stop IOArxCentral`: computers that call in after the release and before the move receive no seat and pause protection until they reach the new Central.
4. Copy the folders `tls` and `keys` and the file `central.db`, with `central.db-wal` and `central.db-shm` when they are there, from `C:\ProgramData\IOArx Central` of the old computer to the same folder of the new computer, in place of the files there. If `central.json` of the old computer holds settings of your own, write them into `central.json` of the new one (Section 4.7).
5. On the new computer, start the service with `sc start IOArxCentral`, open the console, sign in, and activate the license key (Section 6.2).
6. If the new computer takes over the name of Central, point the DNS record to it. Computers reach it at their next call, with the certificate they know.
7. When the computers show **Online** under **Computers**, remove addresses of the old computer under **Settings** › **Server**, and uninstall IOArx Central Monitoring from the old computer (Section 13.5).

Since the database is copied while both services are stopped, Central keeps every event, and the chains of the activity logs continue.

13.5 Uninstall IOArx Central Monitoring

1. If the organization stops using IOArx Business, retire its computers first, so that IOArx Business removes itself from them (Section 13.1). Computers that Central no longer answers keep protecting with their last policy until the period under **Protect without Central for** ends.
2. To use the license key on another Central, release the activation (Section 6.7).
3. In the Windows settings, under **Apps**, uninstall **IOArx Central Monitoring**.

On the Central computer, the uninstaller removes the IOArx Central service and its firewall rule. It keeps the data folder `C:\ProgramData\IOArx Central`, with the database, the certificate and the keys, unless you choose the option to delete the application data. On the computers of administrators, the uninstaller removes the console, which is all that is installed there.

CHAPTER 14

Troubleshooting

14.1 Where to Look First

Table 14.1: Where IOArx Business shows what went wrong

Place	What it shows
The page of the computer in the console	Under **Protection**: **File activity**, **Connections**, **License seat**, a **Note** with the reason when something is off, and **Last seen**. Under **Policy**: whether the newest policy is **Applied**. Under **Activity log**: the chain on the computer and in Central, and what is **Not yet in Central**.
The page **About** of the app on the computer	The version, the computer id, the addresses of Central, the data folder, the records sent and waiting, the chain of hashes, and the **Last problem**.
`ioarx-endpoint status`	What the service says about protection, the connection to Central and the policy (Table 9.7).
`service.log` in the data folder of the computer	What the service did, one line each, starting with the time in milliseconds since January 1, 1970 (UTC). At 2 MB, the file moves to `service.log.old`.
The journal of a Linux computer	The messages of the services: `journalctl -u ioarx-business -u ioarx-monitor`.
`logs\central.log` in the data folder of Central	What the service of Central did, with the time and `INFO`, `WARN` or `ERROR`. At 10 MB, the file moves to `central.log.1`.

14.2 Central

Table 14.2: Problems with Central

Problem	What to do
The installer shows **The IOArx Central Monitoring service could not be set up**, with a reason	Run the installer as an administrator. When the reason says that the service did not start, look for another program on TCP port 9743 with `netstat -ano | findstr :9743`, and read `central.log`.
The console on the Central computer does not connect	Check the service with `sc query IOArxCentral`, and start it with `sc start IOArxCentral`.
Computers or consoles do not reach Central	On the computer, run `Test-NetConnection central.northbridge.example -Port 9743` in PowerShell. When `TcpTestSucceeded` is `False`, check the name in DNS, the firewall rule on Central (Section 4.4) and every firewall between.

Problem	What to do
A computer reports **The secure connection to Central failed**, or a console reports that the certificate of Central is not the one it trusts	Another certificate answers at the address of Central: a proxy or firewall that inspects TLS, or another server. Exempt TCP port 9743 to Central from TLS inspection, and compare the fingerprint with the output of `print-pin` on the Central computer.
Nothing reaches the SIEM	Under **Settings** › **SIEM**, choose **Send a test event**: the page shows the error for each destination. Central keeps the events and tries again with growing pauses.
Central cannot confirm its license	**License** shows when Central last confirmed it. Check that the Central computer reaches `https://ioarx.com` directly or through the proxy under **Settings** › **Network**, then choose **Confirm now** (Section 6.6).

14.3 Enrollment

When a computer does not appear under **Computers**, read the reason on the computer: in the answer of the command `ioarx-endpoint enroll`, under **Last problem** on the page **About** of the app, in the output of `ioarx-endpoint status`, or in `service.log` after `Enrollment was refused`.

Table 14.3: Messages about enrollment

Message	What to do
`This is not an IOArx Business enrollment token.`	Copy the whole token. It starts with `IOXB1.`
`This enrollment token is incomplete. Copy it again from IOArx Central Monitoring.`	Copy the whole token, without line breaks.
`This enrollment token is for a newer version of IOArx Business.`	Install the version of IOArx Business that the **Deployment** page of Central offers.
`This enrollment token is not valid. Copy it again from IOArx Central Monitoring.`	Central does not know the token: it belongs to another Central, or a character changed.
`This enrollment token was revoked. Ask for a new one.`	Create a new token (Section 9.2).
`This enrollment token has expired. Ask for a new one.`	Create a new token.
`This enrollment token was used as often as it allows. Ask for a new one.`	Create a new token, with enough uses.
`Every seat of the license is taken`	Retire computers that are gone, or add seats to the license (Section 6.5).
`No license is active`, `The trial ended`, `The license expired`	Activate or renew the license (Chapter 6).
`Too many attempts. Wait a few minutes and try again.`	Central refused 20 tokens from the network address of the computer within 10 minutes. Wait, and check the token.
`Central could not be reached`, `Central did not answer in time.`	Check the network path to Central (Section 14.2).

Message	What to do
`The secure connection to Central failed`	Exempt TCP port 9743 to Central from TLS inspection (Section 14.2).

Two more cases look like a failed enrollment. A computer installed without a token waits for one: enroll it with `ioarx-endpoint enroll` (Section 9.11). A computer that is still enrolled ignores a new token until Central retires it or its uninstall code is given; it keeps reporting to the Central it belongs to (Section 13.3).

14.4 Computers Offline

A computer shows **Offline** when it has not called in for three heartbeats. Check, in this order:

1. That the computer runs and has a network path to Central, for example through the VPN when it is away from the office.
2. That the service runs: `sc query IOArxBusiness` shows `STATE: 4 RUNNING` on Windows, and `systemctl status ioarx-business ioarx-monitor` shows both services as active on Linux.
3. What the service says: **Last problem** on the page **About** of the app, or the lines `Central could not be reached` in `service.log`.
4. That the computer reaches the port of Central: `Test-NetConnection central.northbridge.example -Port 9743`.

An offline computer keeps protecting with its last policy for the period under **Settings** › **Computers** › **Protect without Central for**, 30 days by default. Its activity log keeps every record, and its other events wait in a queue of up to 20,000, the oldest giving way first. It sends them when it reaches Central again. Central reports a computer that has not called in for 7 days (Table 12.1).

14.5 Incomplete Protection

The column **Protection** under **Computers** names what is missing, and the **Note** on the page of the computer gives the reason.

Table 14.4: States of protection other than Protected

State	Cause	What to do
No seat	The license of Central is not in force; more computers are enrolled than the license covers; the computer has not reached Central for longer than **Protect without Central for** allows; or it never enrolled and its first 72 hours have passed. The app shows **Protection is paused**.	Activate or renew the license (Chapter 6), retire computers that are gone or add seats (Section 6.5), restore the connection to Central, or enroll the computer.

State	Cause	What to do
Files off	The service does not watch file activity.	Choose **Restart the service** under **More actions** on the page of the computer. On Linux, check `systemctl status ioarx-monitor`. When the state stays, read `service.log`.
Network off	The service does not watch connections.	Restart the service. On Linux, check that IOArx Monitor runs and that `sudo nft list table inet ioarx` shows its table.

14.6 Clocks

- Computers sign each request with its time, and Central accepts times within 5 minutes of its own clock. A computer whose clock is off takes the time of Central from the refusal and signs again, so a wrong clock does not keep it from calling in.
- Events carry the time of the computer that recorded them, and Central holds a time ahead of its own clock to at most 10 minutes. Keep staff computers synchronized, so that the timelines of different computers agree.
- The service of a staff computer compares the clock with the time since the start of the computer every 30 seconds. When the clock moves by 5 minutes or more at once, Central receives the sign **The clock jumped**, of high severity, which opens an incident (Table 12.1). Waking from sleep is no jump. A synchronization that corrects a clock by 5 minutes or more at once counts as a jump as well.
- Two-factor sign-in accepts the code of the current 30 seconds and of the 30 seconds before and after, by the clock of Central. A Central clock that is off rejects correct codes.
- The validity of enrollment tokens, the license, sessions and the retention of events count by the clock of Central.

Check the synchronization on Windows and on Linux:

Command Prompt

```
w32tm /query /status
```

Linux

```
timedatectl status
```

14.7 Signing In to the Console

Table 14.5: Problems with signing in

Problem	What to do
Locked until <time> next to an account	Five wrong passwords in a row lock the account for 15 minutes. An administrator with the permission **Manage administrators and roles** chooses **Unlock** in the menu of the account under **Administrators**.

Problem	What to do
A forgotten password	Another administrator with that permission chooses **Set a new password**. Only an Owner changes the account of an Owner; when no Owner can sign in, reset the password on the Central computer (Section 11.11.2).
A lost authenticator app	Another administrator with that permission chooses **Turn off two-factor sign-in**, and the person sets it up again after signing in (Section 5.3).
`Too many attempts. Wait a few minutes and try again.`	Central counted 30 sign-in attempts from the network address of the console within 10 minutes. Wait, then sign in again.
The console reports that the certificate of Central is not the one it trusts	Central was set up again, or another server answers at the address. Compare the fingerprint with the output of `print-pin` on the Central computer before you connect again (Section 5.7).
The console asks to sign in again	The session ended after 30 minutes without use, or after 12 hours (Section 5.8).

APPENDIX A

Command Reference

A.1 IOArx Central Monitoring

Run these commands in a Command Prompt that runs as an administrator. The first two install the computers of the security team; the others run on the Central computer. In the table, `ioarx-central-server.exe` stands for `"C:\Program Files\IOArx Central Monitoring\ioarx-central-server.exe"`.

Table A.1: Commands of IOArx Central Monitoring

Command	What it does
`IOArx-Central-Monitoring_1.0.0_x64-setup.exe /S`	Installs the IOArx Central service and the console without a window, on the Central computer. Run again on a computer with IOArx Central Monitoring, it keeps the role of that computer.
`IOArx-Central-Monitoring_1.0.0_x64-setup.exe /S /CONSOLE`	Installs the console alone without a window, on the computer of an administrator.
`sc query IOArxCentral`	Shows the state of the service.
`sc stop IOArxCentral`, `sc start IOArxCentral`	Stops or starts the service.
`ioarx-central-server.exe print-pin`	Shows the port, the pin and the fingerprint of the certificate of Central.
`ioarx-central-server.exe reset-owner --username <user name>`	Gives an Owner a temporary password, lifts a lock of the account, ends its sessions and turns its two-factor sign-in off.
`ioarx-central-server.exe install`	Sets up the service, the access list of the data folder and the firewall rule for the port of `central.json`, and starts the service, as the installer does. It keeps `central.json` as it is; with `--port <port>`, it changes the port there.
`ioarx-central-server.exe uninstall`	Removes the service and its firewall rule. With `--purge`, it deletes the data folder as well.
`ioarx-central-server.exe run`	Runs Central in the window of the Command Prompt until Ctrl+C, with its log on the screen. Stop the service first.
`ioarx-central-server.exe version`	Shows the version.
`netsh advfirewall firewall show rule name="IOArx Central Monitoring"`	Shows the firewall rule of Central.

The commands of `ioarx-central-server.exe` take `--data <folder>` for a data folder other than `C:\ProgramData\IOArx Central`.

A.2 On Windows Staff Computers

In the table, `ioarx-endpoint.exe` stands for `"C:\Program Files\IOArx Business\ioarx-endpoint.exe"`.

Table A.2: Commands on Windows staff computers

Command	What it does
`IOArx-Business_1.0.0_x64-setup.exe /S /ENROLL=<token>`	Installs IOArx Business without a window and enrolls the computer (Table 9.2). On 32-bit Windows, use the x86 installer.
`ioarx-endpoint.exe enroll --token <token>`	Enrolls a computer that was installed without a token, or whose identity was released (Section 13.3). As an administrator.
`ioarx-endpoint.exe prepare-uninstall --code <uninstall code>`	Gives the uninstall code: the service may be removed, and a new token makes the computer join as a new computer. As an administrator.
`ioarx-endpoint.exe status`	Prints what the service says, as JSON.
`ioarx-endpoint.exe version`	Shows the version.
`"C:\Program Files\IOArx Business\uninstall.exe" /S /CODE=<uninstall code>`	Removes IOArx Business. As an administrator.
`sc query IOArxBusiness`	Shows the state of the service.
`logman query "IOArx Business File Monitor" -ets`	Shows the event trace session through which the service watches file activity.
`Test-NetConnection central.northbridge.example -Port 9743`	Checks, in PowerShell, that the computer reaches the port of Central.
`w32tm /query /status`	Shows the synchronization of the clock.

A.3 On Linux Staff Computers

Table A.3: Commands on Linux staff computers

Command	What it does
`sudo apt install ./ioarx-business_1.0.0_amd64.deb`	Installs IOArx Business on Ubuntu, Debian and the distributions built on them.
`sudo dnf install ./ioarx-business-1.0.0-1.x86_64.rpm`	Installs IOArx Business on Fedora.
`sudo zypper install --allow-unsigned-rpm ./ioarx-business-1.0.0-1.x86_64.rpm`	Installs IOArx Business on openSUSE Tumbleweed.
`sudo ioarx-endpoint enroll --token <token>`	Enrolls the computer.
`sudo ioarx-endpoint prepare-uninstall --code <uninstall code>`	Gives the uninstall code, as on Windows.

Command	What it does
`ioarx-endpoint status`	Prints what the service says, as JSON.
`systemctl status ioarx-monitor ioarx-business`	Shows the state of the services.
`journalctl -u ioarx-business -u ioarx-monitor`	Shows the messages of the services.
`sudo nft list table inet ioarx`	Shows the firewall table of IOArx Monitor.
`sudo IOARX_UNINSTALL_CODE=<uninstall code> apt remove ioarx-business`	Removes IOArx Business; with `dnf remove` or `zypper remove` on Fedora and openSUSE.
`timedatectl status`	Shows the synchronization of the clock.

APPENDIX B

Ports and Addresses

Table B.1: Ports and addresses of IOArx Business

Address	Port	Used by
The addresses of Central under **Settings** › **Server**	TCP 9743, HTTPS	Staff computers and consoles, with the pinned certificate of Central.
`ioarx.com/api/license`	TCP 443, HTTPS	Central: activation and confirmation of the license.
`ioarx.com/updates/business/latest.json`, and the packages it names in `ioarx.com/updates/business/`	TCP 443, HTTPS	Central: new versions of IOArx Business, and the newest installer of IOArx Central Monitoring.
`ioarx.com/updates/central/latest.json`, and the installer it names	TCP 443, HTTPS	The console, when an administrator checks for a new version of IOArx Central Monitoring.
The syslog server under **Settings** › **SIEM**	UDP or TCP, 514 by default	Central, when syslog forwarding is on.
The webhook address under **Settings** › **SIEM**	The port of the address	Central, when the webhook is on.
`clients2.google.com/service/update2/crx`	TCP 443, HTTPS	Chrome: installation and updates of IOArx for Browsers (Business).
`edge.microsoft.com/extensionwebstorebase/v1/crx`	TCP 443, HTTPS	Edge: installation and updates of IOArx for Browsers (Business).
`\\.\pipe\IOArxBusiness`	Local	The app and the browsers on a Windows computer, to the service.
`/run/ioarx-business.sock`	Local	The app and the browsers on a Linux computer, to the service.

APPENDIX C

File Locations

Table C.1: Files of IOArx Business on Windows staff computers

Path	What it is
`C:\Program Files\IOArx Business\ioarx-endpoint.exe`	The service, the command for administrators, and the native messaging host of the browsers.
`C:\Program Files\IOArx Business\IOArx Business.exe`	The app.
`C:\Program Files\IOArx Business\uninstall.exe`	The uninstaller.
`C:\Program Files\IOArx Business\browser\`	The manifests of the native messaging host, `chromium.json` and `firefox.json`, and `written.json`, the list of browser policies that IOArx Business wrote.
`C:\Program Files\IOArx Business\extension\ioarx-business.xpi`	The package of IOArx for Browsers (Business) for Firefox, when present (Section 10.5).
`C:\ProgramData\IOArx Business\`	The data folder (Table C.2).

Table C.2: The data folder of IOArx Business, `C:\ProgramData\IOArx Business` or `/var/lib/ioarx-business`

File	What it holds
`device.json`	The identity of the computer: its id, its key, the secret behind its uninstall code, and the addresses and pins of Central.
`enroll.json`	An enrollment token that waits for the service.
`policy.json`	The last policy from Central.
`license.json`	What Central last said about the seat of the computer.
`audit.jsonl`	The activity log, chained by hashes.
`upload.json`	How far Central has received the activity log.
`spool.jsonl`	Other events that wait to be sent.
`requests.json`	The requests for access of the people at the computer.
`locks.json`	The locks in force, with the access each file or folder had before.
`browsers.json`	The browsers from which IOArx for Browsers (Business) connected.
`retired.json`	The mark of a retirement by Central.
`released.json`	The mark that the uninstall code was given.
`updates\`	Update packages from Central.

File	What it holds
`service.log`, `service.log.old`	What the service did, for support.

On Linux, Table 9.6 lists the files of the packages. The browser policies on Linux are listed in Table 10.2.

Table C.3: Files of IOArx Central Monitoring

Path	What it is
`C:\Program Files\IOArx Central Monitoring\IOArx Central Monitoring.exe`	The console.
`C:\Program Files\IOArx Central Monitoring\ioarx-central-server.exe`	The service of Central and its commands (Appendix A).
`C:\Program Files\IOArx Central Monitoring\uninstall.exe`	The uninstaller.
`C:\ProgramData\IOArx Central\`	The data folder of Central (Table 4.2), on the Central computer only.
`C:\ProgramData\IOArx Central\logs\central.log`	The log of the service, on the Central computer only.

The computers of administrators with the console alone hold the program folder only.

APPENDIX D

Roles and Permissions

The role Owner holds every permission. The role Administrator holds every permission except **Manage the license**, and cannot change the accounts of Owners. The table lists, for each permission as the page **Roles** names it, the built-in roles that hold it.

Table D.1: Permissions of the built-in roles

Permission	Built-in roles that hold it
Overview	
See the overview	Owner, Administrator, Security Analyst, Helpdesk, Auditor, Privacy Officer
Make reports	Owner, Administrator, Security Analyst, Auditor, Privacy Officer
Investigation	
Investigate events	Owner, Administrator, Security Analyst, Auditor, Privacy Officer
Export events	Owner, Administrator, Security Analyst
See the names behind pseudonyms	Owner, Administrator, Privacy Officer
Response	
See incidents	Owner, Administrator, Security Analyst, Auditor, Privacy Officer
Work on incidents	Owner, Administrator, Security Analyst
Answer approval requests and requests for access	Owner, Administrator, Security Analyst, Helpdesk
Computers	
See computers	Owner, Administrator, Security Analyst, Helpdesk, Auditor
Manage computers	Owner, Administrator, Helpdesk
Lock files and folders, isolate computers and stop AI agents	Owner, Administrator, Security Analyst
People	
See people	Owner, Administrator, Security Analyst, Helpdesk, Auditor, Privacy Officer
Manage people	Owner, Administrator, Helpdesk
AI usage	
See the AI inventory	Owner, Administrator, Security Analyst, Auditor
See browser security	Owner, Administrator, Security Analyst, Auditor

Permission	Built-in roles that hold it
Access profiles	
See access profiles	Owner, Administrator, Security Analyst, Auditor, Privacy Officer
Change access profiles	Owner, Administrator
Deployment	
Enroll computers	Owner, Administrator, Helpdesk
Administration	
See administrators	Owner, Administrator, Auditor, Privacy Officer
Manage administrators and roles	Owner, Administrator
Read the audit log	Owner, Administrator, Auditor, Privacy Officer
Central	
Manage the license	Owner
Manage updates	Owner, Administrator
Change the settings of Central	Owner, Administrator

APPENDIX E

Glossary

Table E.1: Terms of IOArx Business

Term	Meaning
Access profile	The rules and settings that a computer enforces: files and folders, secrets, network, AI agents, detection, prompts, locks, browser, privacy and computer options.
Activity log	The record of every decision on a computer, each entry chained to the one before by its SHA-256 hash.
AI agent	A program that acts on its own with the help of an AI model, such as a coding assistant that reads files and runs commands.
Approval request	The question that a paused AI agent waits on, when a rule says Ask and an administrator answers.
Ask, Allow, Block	What a rule does with an access: pause the AI agent for an answer, let it go on, or stop it.
Central	IOArx Central, the service `IOArxCentral` that holds the database of the organization and talks to every computer.
Console	The app of IOArx Central Monitoring with which administrators work with Central.
Enrollment	The first contact of a computer with Central, with which it joins the organization and takes a seat.
Enrollment token	The text, starting with `IOXB1.`, that carries the addresses of Central, the pin of its certificate, the organization and a secret, and lets computers enroll.
Fingerprint	The SHA-256 hash of the certificate of Central, in 16 groups of four characters, for comparison by eye.
Group	A set of computers with an access profile, which they follow unless the computer or its person has a profile of its own.
Heartbeat	The regular call of a computer to Central, every 30 seconds by default.
Incident	A case that Central opens for an event of high or critical severity, with the related events, notes and changes.
Isolation	A state of a computer in which every AI agent is stopped at its first file access or connection.
Lock	A file or folder that no program of a signed-in person can open until an administrator unlocks it.
Native messaging host	The program through which a browser extension talks to a program of the computer; for IOArx for Browsers (Business), `com.ioarx.business`.
Owner	The role with every permission. At least one active administrator always holds it.

Term	Meaning
Pin	The SHA-256 hash of the certificate of Central, in base64url, by which computers and consoles recognize Central.
Policy	The access profile of a computer as Central compiles it for that computer, with a version number.
Pseudonym	A stand-in for the name of a person, such as Person 7F3A, that administrators without the permission **See the names behind pseudonyms** see when pseudonyms are on.
Receipt	A summary of the activity log of a computer, signed with its key, that Central compares with the records it holds.
Request for access	A request from a person, made in the app, to let an AI agent read or change a file or folder, or reach a host.
Retire	To take a computer out of the organization: its seat is freed and IOArx Business removes itself.
Role	A named set of permissions given to administrators.
Scope	The groups of computers that an administrator may see and manage.
Seat	The right of one enrolled computer to protection under the license.
Tamper protection	The setting that keeps the service from being stopped or uninstalled without an administrator of Central.
Uninstall code	The code of one computer that allows IOArx Business to be removed from it.
Update key	The key with which IOArx signs every package of IOArx Business.