Identity and access management: selection criteria grid for a terminal

For: IT managers, CIOs and security leads of a container or multipurpose terminal choosing or reviewing identity and access tools

Write the names of the tools on your shortlist at the top of the empty columns. For each line, ask the publisher the question, then ask to see it in a demonstration or in the documentation, and write what you saw. Give each line a weight for your terminal before the first demonstration, not after. The grid does not score the tools for you: the lines that matter most are the ones your gate, yard and vendors depend on.

Scope. Identity and access management (IAM) decides who is who, what each person may open and how they prove it. In a terminal it covers office staff, but also shift workers at the gate and in the yard, contractors, vendor engineers who support the terminal operating system (TOS) and the cranes, and the partners whose systems call the terminal's interfaces. This grid helps compare tools for that job. It is not a product test and Port Cyber Alliance does not certify tools.

Seven families, 29 criteria

• **D · Directory**: One place that says who exists, with what role and until when, and that the other systems trust.

• **S · Single sign-on and federation**: One logon for many applications through open standards, so that closing one account closes all access.

• **M · Multi-factor authentication**: A second factor everywhere it is asked, phishing-resistant where it matters most.

• **P · Privileged access**: Administrators and vendor engineers reach critical servers through one controlled, recorded path.

• **J · Joiners, movers, leavers**: Employees, contractors and vendor staff get access on arrival, change it when they change job, and lose it the day they leave.

• **G · Gate, yard and shared terminals**: Shift workers on shared screens, in cabins and at the gate, each with their own identity, fast enough for the work.

• **R · Running it**: Where it runs, what happens when a link is down, where its logs go, and how you leave it.

Answer per tool

• shown · seen working in a demonstration or a test, with the date

• documented · written in the publisher's documentation, not seen yet

• partial · only with an add-on, a script, a higher edition or a workaround: write which

• no · not available

Weight per line (set before the first demonstration)

• must · a no here ends the evaluation

• should · counts in the comparison

• nice to have

Comparison sheet · terminal: _____ · date: _____

Write shown / documented / partial / no in each tool column. No total: read the « must » lines first.

Criterion	Weight	Tool 1: _____	Tool 2: _____	Tool 3: _____
D1 · One source of truth for people				
D2 · Groups and roles that match the terminal				
D3 · A complete export of who has access to what				
D4 · Lockout and password rules set centrally				
S1 · Open standards for single sign-on				
S2 · What to do with applications that know no standard				
S3 · Sessions that end				
S4 · Partners and their own logons				
M1 · A second factor where the rules ask for one				
M2 · Phishing-resistant factors				
M3 · Weaker factors under control				
M4 · Lost factor, without a back door				
P1 · Admin accounts apart from daily accounts				
P2 · Privilege given for a job, then taken back				
P3 · One recorded path for vendor engineers				
P4 · Shared technical passwords kept in a vault				
J1 · Every contractor has a sponsor and an end date				
J2 · Leavers lose everything the same day				
J3 · Movers do not keep their old rights				
J4 · Regular access reviews				
J5 · Accounts nobody uses				
G1 · No shared account on a shared screen				
G2 · Fast switch between workers				
G3 · Screens that lock themselves				
G4 · Working when the link is down				
R1 · Where it runs				
R2 · Logs that reach your SIEM				
R3 · The identity system is itself protected				
R4 · A way out				

D · Directory

One place that says who exists, with what role and until when, and that the other systems trust.

D1 · One source of truth for people *(IMO Rev.4 3.5.3.1 · CISA/NSA ESF IAM guide (identity governance))*

Ask: Can the tool be the one directory for staff, contractors and vendor engineers, or read them from the directory you already have (for example over LDAP or from the HR system), without a second list kept by hand?

Why: IMO Rev.4 asks for unique credentials for all users (3.5.3.1). The CISA and NSA IAM guide for administrators (March 2023) starts with identity governance: knowing every identity and who is responsible for it. Two lists kept by hand drift apart, and the leaver stays in one of them.

Ask to see: [ ] Where each kind of user (staff, contractor, vendor) is created, shown in the demonstration · [ ] What happens in the tool when a person is removed from the source directory

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

D2 · Groups and roles that match the terminal *(33 CFR 101.650(a)(5) · NIS2 Art. 21(2)(i))*

Ask: Can access be given by role (gate clerk, planner, crane technician, TOS administrator, vendor support) rather than person by person, and can one person hold a role for a limited time?

Why: 33 CFR 101.650(a)(5) requires least privilege for administrator and other privileged accounts. NIS2 Art. 21(2)(i) lists access control policies among the measures every essential or important entity takes. Roles are how least privilege stays true when people change shifts and roles.

Ask to see: [ ] The role list configured for a test site, with the rights of each role · [ ] A role given with an end date, and what happens on that date

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

D3 · A complete export of who has access to what *(33 CFR 101.650(b)(3) · AA23-278A, misconfiguration 9)*

Ask: Can you export, at any time, the list of accounts with their roles, their last logon and their end date, in a format a spreadsheet opens?

Why: 33 CFR 101.650(b)(3) requires an accurate inventory of network-connected systems; the people who can reach them are part of that picture. The NSA/CISA advisory AA23-278A lists poor credential hygiene (misconfiguration 9). An access review starts from that export.

Ask to see: [ ] An export from the test site, opened in a spreadsheet · [ ] The fields it holds (last logon, end date, role, sponsor)

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

D4 · Lockout and password rules set centrally *(33 CFR 101.650(a)(1)-(3) · AA23-278A, misconfiguration 1)*

Ask: Are lockout after repeated failures, password strength and the change of initial passwords set once in the tool and applied to every application behind it?

Why: 33 CFR 101.650(a)(1) to (a)(3) require automatic lockout after repeated failed logins, default passwords changed before use, and a minimum password strength. AA23-278A puts default configurations first in its list.

Ask to see: [ ] The lockout and password settings page · [ ] What a new account must do at its first logon

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

S · Single sign-on and federation

One logon for many applications through open standards, so that closing one account closes all access.

S1 · Open standards for single sign-on ***(CISA/NSA ESF IAM guide (identity federation and single sign-on))***

Ask: Which standards does the tool speak to applications: OpenID Connect, OAuth 2.0, SAML 2.0, LDAP, Kerberos? Which of your applications (TOS client, gate system, mail, maintenance software, portals) speak one of them?

Why: The CISA and NSA IAM guide for administrators (March 2023) covers identity federation and single sign-on as one of its five areas. With open standards, an account closed in one place is closed for every application behind it, and the terminal can change tool later.

Ask to see: [ ] The list of protocols in the documentation · [ ] Your own list of applications, each marked with the standard it supports, or « none »

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

S2 · What to do with applications that know no standard ***(33 CFR 101.650(a)(7))***

Ask: For the old applications that only have their own user list (some TOS clients, OCR consoles, crane maintenance tools), what does the tool offer: account sync, a gateway in front of the application, or nothing?

Why: An application outside single sign-on keeps its own accounts, and its leavers are the ones forgotten. 33 CFR 101.650(a)(7) requires credentials removed or revoked when a user leaves the organisation, in every system.

Ask to see: [ ] The answer for each of your applications that has no standard · [ ] The written procedure for the ones that stay outside

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

S3 · Sessions that end ***(NIST SP 800-207, section 2.1, tenet 3)***

Ask: Can session length and idle timeout be set per application, and can an administrator end all sessions of one person at once?

Why: NIST SP 800-207 (zero trust) grants access to each resource per session (tenet 3). When a badge is lost or a person is dismissed, ending every open session matters as much as disabling the account.

Ask to see: [ ] The session settings per application · [ ] « End all sessions » for one test user, shown in the demonstration

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

S4 · Partners and their own logons ***(CISA/NSA ESF IAM guide (identity federation))***

Ask: Can staff of a partner (shipping line, haulier, customs broker) log in with their own company account through federation, with the terminal still deciding what they may see?

Why: The CISA and NSA IAM guide covers identity federation. Federation removes shared partner accounts, but only if the terminal keeps the rights on its side and can cut one partner off.

Ask to see: [ ] A federated test partner, its rights, and how it is cut off

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

M · Multi-factor authentication

A second factor everywhere it is asked, phishing-resistant where it matters most.

M1 · A second factor where the rules ask for one *(33 CFR 101.650(a)(4) · NIS2 Art. 21(2)(j) · IMO Rev.4 3.5.3.2)*

Ask: Can the tool ask for a second factor on every password-protected application and every remote access, and record the exceptions with their compensating control?

Why: 33 CFR 101.650(a)(4) requires multi-factor authentication on password-protected IT and on remotely accessible OT, with documented compensating controls where it is not feasible. NIS2 Art. 21(2)(j) names multi-factor or continuous authentication. IMO Rev.4 asks for it in 3.5.3.2.

Ask to see: [ ] The policy that decides when the second factor is asked · [ ] Where exceptions and their compensating control are written

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

M2 · Phishing-resistant factors *(CISA phishing-resistant MFA fact sheet · NIST SP 800-63B-4, 2.2, 2.3, 3.2.5)*

Ask: Does the tool support phishing-resistant authenticators: FIDO2/WebAuthn security keys and passkeys, or smart cards (PKI)? Can they be required for administrators and remote access?

Why: CISA's fact sheet (October 2022) names FIDO/WebAuthn and PKI-based authentication as phishing-resistant and urges them as a high priority. NIST SP 800-63B-4 requires phishing resistance at AAL3 and requires verifiers to offer a phishing-resistant option at AAL2 (section 3.2.5 defines it).

Ask to see: [ ] A logon with a security key or a passkey, shown · [ ] The policy that requires it for the administrator role

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

M3 · Weaker factors under control *(CISA phishing-resistant MFA fact sheet · NIST SP 800-63B-4, 3.1.3.3 · AA23-278A, misconfiguration 7)*

Ask: If push notifications or codes are kept for some users, does the tool offer number matching, limit repeated push requests, and let you switch off SMS and voice codes?

Why: CISA's fact sheet describes push bombing and SIM swap attacks and recommends number matching where factors are not phishing-resistant. NIST SP 800-63B-4 marks authentication over the public telephone network as restricted (3.1.3.3). AA23-278A lists weak or misconfigured MFA methods as misconfiguration 7.

Ask to see: [ ] The factor settings page, with SMS and voice switched off · [ ] What a user sees after several refused push requests

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

M4 · Lost factor, without a back door *(CISA/NSA ESF IAM guide (multifactor authentication))*

Ask: When a worker loses a key or a phone during a night shift, how do they get back in, and who checks it is really them before a new factor is registered?

Why: A recovery path that only needs a phone call to the help desk undoes the second factor. The CISA and NSA IAM guide covers MFA and the hardening of the processes around it.

Ask to see: [ ] The written recovery procedure, with who approves it out of office hours · [ ] A recovery shown for a test user

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

P · Privileged access

Administrators and vendor engineers reach critical servers through one controlled, recorded path.

P1 · Admin accounts apart from daily accounts *(33 CFR 101.650(a)(6) · AA23-278A, misconfiguration 2)*

Ask: Can administrators have a separate, named admin identity, with its own stronger rules, kept apart from the account they use for mail and the web?

Why: 33 CFR 101.650(a)(6) asks that users keep separate credentials on critical IT and OT systems. AA23-278A names improper separation of user and administrator privilege as misconfiguration 2.

Ask to see: [ ] A test administrator with two identities, and the rules on each

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

P2 · Privilege given for a job, then taken back *(33 CFR 101.650(a)(5))*

Ask: Can administrator rights be requested, approved and granted for a stated job and a limited time, then removed automatically?

Why: 33 CFR 101.650(a)(5) requires least privilege for administrator and other privileged accounts. Rights that are only there during the job cannot be used the rest of the year.

Ask to see: [ ] A request, its approval and the automatic removal, shown · [ ] The record of who held which right and when

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

P3 · One recorded path for vendor engineers *(33 CFR 101.650(f)(3) · CISA remote access guide (June 2023))*

Ask: Can vendor and support engineers reach the TOS servers, crane systems or gate servers only through one gateway that checks their identity and second factor and records the session?

Why: 33 CFR 101.650(f)(3) requires the owner or operator to monitor and document all third-party remote connections. The CISA-led Guide to Securing Remote Access Software (June 2023) recommends knowing and allowlisting the remote access tools in use.

Ask to see: [ ] A vendor session through the gateway, and its record · [ ] How long session records are kept, and who reads them

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

P4 · Shared technical passwords kept in a vault *(AA23-278A, misconfiguration 9 · IMO Rev.4 3.5.3.1)*

Ask: Where a system only has one built-in admin password (a switch, a PLC engineering station, a database), can the tool keep it in a vault, show who took it, and change it after use?

Why: AA23-278A lists poor credential hygiene (misconfiguration 9). IMO Rev.4 asks for unique credentials (3.5.3.1): where a device cannot have them, knowing who used the shared one is the next best thing.

Ask to see: [ ] The vault entry of a test device, with its check-out history · [ ] The password change after check-in, shown

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

J · Joiners, movers, leavers

Employees, contractors and vendor staff get access on arrival, change it when they change job, and lose it the day they leave.

J1 · Every contractor has a sponsor and an end date (33 CFR 101.650(a)(7))

Ask: Can every contractor or vendor account carry a sponsor inside the terminal and an end date, and is it disabled on that date unless the sponsor renews it?

Why: 33 CFR 101.650(a)(7) requires credentials removed or revoked when a user leaves the organisation. A contractor rarely « leaves » in the HR system: the end date is the only reliable trigger.

Ask to see: [ ] A contractor account with sponsor and end date · [ ] What the sponsor receives before the end date

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

J2 · Leavers lose everything the same day (33 CFR 101.650(a)(7) · CISA remote access guide (June 2023))

Ask: When a person leaves, does one action disable the directory account, end open sessions, revoke registered factors and flag the accounts in applications outside single sign-on?

Why: 33 CFR 101.650(a)(7) requires credentials removed or revoked on leaving. The CISA-led remote access guide recommends auditing the directory for inactive and obsolete accounts.

Ask to see: [ ] The leaver action on a test user, and what it changed · [ ] The list of applications it does not reach

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

J3 · Movers do not keep their old rights (33 CFR 101.650(a)(5))

Ask: When a gate clerk becomes a planner, or a technician moves to another site, are the rights of the old role removed when the new one is given?

Why: 33 CFR 101.650(a)(5) requires least privilege. Rights that pile up with each move are a quiet breach of it, and a gift to anyone who takes over that account.

Ask to see: [ ] A role change on a test user, before and after

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

J4 · Regular access reviews (NIS2 Art. 21(2)(i) · CISA/NSA ESF IAM guide (identity governance, auditing))

Ask: Can the tool send each manager or sponsor the list of their people's access to confirm or remove, and keep the answers?

Why: NIS2 Art. 21(2)(i) lists human resources security and access control policies. The CISA and NSA IAM guide puts identity governance and IAM auditing among its five areas. A review with a written answer is evidence.

Ask to see: [ ] A review campaign on the test site, and its result file

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

J5 · Accounts nobody uses (CISA remote access guide (June 2023) · AA23-278A, misconfiguration 9)

Ask: Does the tool list accounts that have not logged in for a set number of days, and can it disable them automatically?

Why: The CISA-led remote access guide recommends auditing for inactive and obsolete accounts. AA23-278A lists poor credential hygiene (misconfiguration 9).

Ask to see: [ ] The inactive-account report on the test site

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

G · Gate, yard and shared terminals

Shift workers on shared screens, in cabins and at the gate, each with their own identity, fast enough for the work.

G1 · No shared account on a shared screen ***(IMO Rev.4 3.5.3.1)***

Ask: On a gate lane PC, a yard tablet or a control-room console used by several people per day, does each worker log in as themselves, or is there one shared account?

Why: IMO Rev.4 asks for unique credentials for all users (3.5.3.1). A shared account cannot be closed for one leaver and does not say who did what at the gate.

Ask to see: [ ] The list of shared screens and the account each one uses today · [ ] How the tool handles several users on one device, shown

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

G2 · Fast switch between workers ***(NIST SP 800-207, section 2.1, tenet 3)***

Ask: How long does it take one worker to leave a shared screen and the next one to log in, with the second factor, wearing gloves? Can a badge tap plus a PIN do it?

Why: A logon that slows a lane at shift change gets bypassed: the screen stays logged in. NIST SP 800-207 grants access per session (tenet 3): the switch must be fast enough to be used every time.

Ask to see: [ ] The switch timed on a real shared screen, at shift change, by the people who use it

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

G3 · Screens that lock themselves ***(NIST SP 800-207, section 2.1, tenet 3)***

Ask: Can shared screens lock after a short idle time, and close the session when a worker walks away, without losing the work of the next one?

Why: NIST SP 800-207 grants access per session (tenet 3). An unlocked lane PC is an open session for whoever stands in front of it.

Ask to see: [ ] The idle lock setting for shared screens, shown on a device

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

G4 · Working when the link is down ***(33 CFR 101.650(a)(4))***

Ask: If the link to a cloud identity service or to the head office is down, can gate and yard staff still log in, and for how long? What is the documented fallback?

Why: The gate works around the clock. 33 CFR 101.650(a)(4) allows documented compensating controls where multi-factor authentication is not feasible: a link outage is the case to plan in writing, not at 3 a.m.

Ask to see: [ ] The publisher's documented behaviour when the identity service is unreachable · [ ] Your written fallback for the gate and the yard

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

R · Running it

Where it runs, what happens when a link is down, where its logs go, and how you leave it.

R1 · Where it runs *(NIS2 Art. 21(2)(d))*

Ask: Is the tool a cloud service, software you host, or both? Who operates it, who patches it, in which country is the data held?

Why: NIS2 Art. 21(2)(d) covers supply chain security, including the security aspects of the relationship with each direct supplier. The identity system becomes one of the most critical suppliers of the terminal.

Ask to see: [ ] The hosting options and data locations in the documentation · [ ] Who patches it, and how fast, in writing

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

R2 · Logs that reach your SIEM *(33 CFR 101.650(c)(1) · CISA/NSA ESF IAM guide (auditing and monitoring))*

Ask: Does the tool log logons, failures, factor changes, role changes and administrator actions, and send them to your log store or SIEM in a documented format?

Why: 33 CFR 101.650(c)(1) requires logs to be securely captured, stored and protected. The CISA and NSA IAM guide names IAM auditing and monitoring as one of its five areas.

Ask to see: [ ] A sample of the log lines for a logon and a role change · [ ] The forwarding settings to your SIEM

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

R3 · The identity system is itself protected *(CISA/NSA ESF IAM guide (environmental hardening))*

Ask: How are the tool's own administrators protected (phishing-resistant factor, separate accounts), and how is a compromise of the tool detected?

Why: Whoever controls the identity system controls every account behind it. The CISA and NSA IAM guide covers environmental hardening of the identity infrastructure.

Ask to see: [ ] The admin accounts of the tool and their factors · [ ] The alerts on changes to its configuration

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

R4 · A way out *(Licence of the software · line S1)*

Ask: Can users, groups, roles and configuration be exported in a documented format, so the terminal can change tool or host later? Under which licence is the software published?

Why: Open standards (line S1) and a full export keep the terminal free to change. The licence decides what you may run, change and redistribute: read it before you build on the tool.

Ask to see: [ ] A full export from the test site · [ ] The licence text, read

Weight: [ ] must [ ] should [ ] nice Tool 1: _____ Tool 2: _____ Tool 3: _____

Tool categories and open-source examples

Examples only: public open-source projects, in alphabetical order inside each category, described in their publisher's own words, with the licence their repository declares (read on 11 November 2026). Not a ranking, not a recommendation, not a test. Commercial products exist in every category and are not listed.

Directories

Hold the list of people and groups that other systems trust, usually over LDAP or Kerberos. The « LDAP » of the 1990s is still here, often behind a newer layer.

• **FreeIPA**: « Identity, Policy, Audit »: manage Linux users and client hosts in your realm from one central location · licence: GPL-3.0 · https://www.freeipa.org/

• **lldap**: « Light LDAP implementation » · licence: GPL-3.0 · https://github.com/lldap/lldap

• **OpenLDAP**: « an open source implementation of the Lightweight Directory Access Protocol » · licence: OpenLDAP Public License (see the project) · https://www.openldap.org/

• **Samba**: an open source implementation of the SMB and Active Directory protocols for Linux and UNIX-like systems · licence: GPL-3.0 · https://www.samba.org/

Identity providers and single sign-on

Give one logon to many applications over OpenID Connect, OAuth 2.0 or SAML, often with multi-factor authentication built in.

• **authentik**: « The authentication glue you need. » · licence: see the repository's licence file · https://goauthentik.io/

• **Authelia**: « The Single Sign-On Multi-Factor portal for web apps. » · licence: Apache-2.0 · https://www.authelia.com/

• **Keycloak**: « Open Source Identity and Access Management For Modern Applications and Services » · licence: Apache-2.0 · https://www.keycloak.org/

• **Logto**: « Authentication and authorization infrastructure for SaaS and AI apps, built on OIDC and OAuth 2.1 with multi-tenancy, SSO, and RBAC. » · licence: MPL-2.0 · https://logto.io/

• **Ory Hydra and Ory Kratos**: Hydra: « OpenID Certified™ OpenID Connect and OAuth2.1 provider that integrates with your user management through headless APIs »; Kratos: « Headless cloud-native authentication and identity management » · licence: Apache-2.0 · https://github.com/ory

• **ZITADEL**: « Identity infrastructure, simplified for you. » · licence: AGPL-3.0 · https://zitadel.com/

Privileged and remote access gateways

Put one controlled, recorded path in front of servers and consoles for administrators and vendor engineers.

• **Apache Guacamole**: « a clientless remote desktop gateway. It supports standard protocols like VNC, RDP, and SSH. » · licence: Apache-2.0 · https://guacamole.apache.org/

• **JumpServer**: « an Open-source Privileged Access Management (PAM) platform » · licence: GPL-3.0 · https://github.com/jumpserver/jumpserver

Phishing-resistant factors

Not a product but a family of standards: FIDO2/WebAuthn security keys and passkeys, and smart cards (PKI). Check that the identity provider, the browsers and the shared screens of the terminal all support the one you choose.

Sources (public, dated)

eCFR, 33 CFR 101.650, Cybersecurity measures (US Coast Guard rule), in force since 16 July 2025, read on 11 November 2026. https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F/section-101.650

IMO, MSC-FAL.1/Circ.3/Rev.4, Guidelines on maritime cyber risk management, 28 May 2026. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

Directive (EU) 2022/2555 (NIS2), Article 21(2), 14 December 2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

NIST SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management, July 2025. https://csrc.nist.gov/pubs/sp/800/63/b/4/final

NIST SP 800-207, Zero Trust Architecture, August 2020. https://csrc.nist.gov/pubs/sp/800/207/final

CISA, Implementing Phishing-Resistant MFA (fact sheet), October 2022. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

CISA and NSA (Enduring Security Framework), Identity and Access Management Recommended Best Practices Guide for Administrators, 21 March 2023. https://www.cisa.gov/news-events/alerts/2023/03/21/cisa-and-nsa-release-enduring-security-framework-guidance-identity-and-access-management

NSA and CISA, advisory AA23-278A, Top Ten Cybersecurity Misconfigurations, 5 October 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a

CISA, NSA, FBI, MS-ISAC and INCD, Guide to Securing Remote Access Software, 6 June 2023. https://www.cisa.gov/resources-tools/resources/guide-securing-remote-access-software

Licence

Creative Commons Attribution 4.0 International (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/ . You may copy, adapt and share this grid, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/resources/tools-directory/iam-tools-analysis/ . Generic: no terminal, port or client is named, no figure is invented, no tool is ranked or priced. This grid is not legal advice. Port Cyber Alliance does not certify tools or terminals.