Admin By Request
ZERO TRUST PLATFORM

Web Access Management

Feature Breakdown

Platform support:
The initial release of Web Access Management is available on Windows endpoints only. Mac and Linux support are not yet available but are planned for a future release.

1. Browser Lockdown

Define which browsers are allowed, and what version they need to be.

Not all browsers are equal from a security standpoint, and unmanaged browser usage means outdated or unsupported software can slip through. Browser Lockdown lets you specify exactly which browsers are permitted on managed endpoints, and set a minimum version for each one.

Browsers that don't meet your requirements are blocked before they can be used. You can manage Chrome, Edge, Firefox, and Internet Explorer independently, and apply a separate rule for in-app browsers and embedded webviews.

CONFIGURATION LOCATION
Portal path: Web Access Settings > Lockdown > Browsers

CONTROLS
The Browsers tab displays a table with one row per supported browser:

- Browser: Chrome, Edge, Firefox, Internet Explorer, Non-browsers (in-app browsers)
- Min. Version: free-text input per browser; leave empty to apply no minimum
- Allowed: ON/OFF toggle per browser (ON = permitted; OFF = blocked)
- Save button applies changes to all rows in the panel

BEHAVIOR
- Each browser row is configured independently.
- When Allowed is OFF for a browser, that browser is blocked on the endpoint regardless of version.
- When Allowed is ON and a Min. Version is set, only that version or higher is permitted.
- When Min. Version is empty and Allowed is ON, no version restriction is enforced.
- The Non-browsers row controls whether in-app browsers (such as embedded webviews) are permitted.
- Configuration is persisted at tenant level and distributed to endpoints via policy payload.

2. Blocked Sites Enforcement

Deny access to specific websites at the endpoint, on or off the network.

Blocked site rules stop users from reaching destinations you've explicitly disallowed, with enforcement happening on the device itself rather than at a network choke point. Rules apply regardless of whether the user is in the office, working from home, or connected from somewhere else entirely.

Rules are defined by root URL, optionally scoped to a subpath. Each one can carry a custom blocking message for users who hit it, and can be individually flagged for audit logging. Blocked rules always take priority over pre-approved rules, so a site that appears on both lists stays blocked.

CONFIGURATION LOCATION
List page: Web Access Settings > Site Control > Blocked
Create/Edit page: Web Access Settings > Site Control > Blocked > New entry / row selection

LIST PAGE CONTROLS

- Enabled: global ON/OFF toggle; when OFF, no blocked site rules are enforced
- Grid columns: URL, Log (ON/OFF indicator)
- New entry button: opens the Create page
- Export buttons: PDF, XLSX, CSV

CREATE/EDIT CONTROLS
The Browsers tab displays a table with one row per supported browser:

- Root URL (required): domain or domain + subpath; scheme not required
- Log to auditlog: ON/OFF toggle per rule
- Blocking message (optional): message shown to the user when access is blocked
- Internal comments (optional): not visible to end users

BEHAVIOR

- Root URL is normalized on save: whitespace trimmed, host lowercased, trailing slash removed.
- Normalization prevents duplicates caused by minor formatting differences.
- Blocking message is optional; when configured it is shown to the user at the point of block.
- Rules and the global enabled flag are distributed via endpoint policy API.
- Blocked site rules take priority over pre-approved site rules.

3. Browsing Permission Controls

Set the baseline for what users can access, and how much flexibility they have.

Browsing permission controls let you decide whether users can browse freely, or whether access is restricted to sites you've explicitly approved. When open browsing is off, users can only reach sites on your pre-approved list.

If you want to allow access to blocked sites under some conditions, you can require users to request approval before proceeding, provide a reason, or both. Approvals go through the portal, giving admins visibility and a documented decision trail before access is granted.

CONFIGURATION LOCATION
Portal path: Web Access Settings > Authorization > Browsing

CONTROLS
- Allow Browsing toggle
- Allow Blocked Sites toggle (available when Allow Browsing is ON)
- Require Approval toggle (available when Allow Blocked Sites is ON)
- Require Reason toggle (available when Allow Blocked Sites is ON)
- Save button

BEHAVIOR
- Allow Browsing ON: users can browse the internet normally.
- Allow Browsing OFF: users can only access sites on the pre-approved list. Allow Blocked Sites is disabled.
- Allow Blocked Sites ON: users may access sites on the blocked list, subject to any Require Approval or Require Reason settings.
- Allow Blocked Sites OFF: blocked list sites remain inaccessible.
- Require Approval ON: a portal admin must approve access before a blocked site can be opened. Approval grants four hours of access before the restriction automatically reasserts itself.
- Require Reason ON: the user must provide a reason before accessing a blocked site; an empty reason field rejects the request.
- Toggle states are persisted at tenant level. After a page refresh, values reflect the saved backend state.

4. Pre-approved Sites

Let trusted destinations through without generating an approval request.

Blocked site rules stop users from reaching destinations you've explicitly disallowed, with enforcement happening on the device itself rather than at a network choke point. Rules apply regardless of whether the user is in the office, working from home, or connected from somewhere else entirely.

Rules are defined by root URL, optionally scoped to a subpath. Each one can carry a custom blocking message for users who hit it, and can be individually flagged for audit logging. Blocked rules always take priority over pre-approved rules, so a site that appears on both lists stays blocked.

CONFIGURATION LOCATION
List page: Web Access Settings > Site Control > Pre-approved
Create/Edit page: Web Access Settings > Site Control > Pre-approved > New entry / row selection

LIST PAGE CONTROLS
- Enabled: global ON/OFF toggle; when OFF, no pre-approved site rules are applied
- Grid columns: URL, Log (ON/OFF indicator)
- New entry button: opens the Create page
- Export buttons: PDF, XLSX, CSV

CREATE/EDIT CONTROLS

- Root URL (required): domain or domain + subpath; scheme not required
- Log to auditlog: ON/OFF toggle per rule
- Internal comments (optional)

BEHAVIOR

- Root URL accepts scheme-less input and is normalized on save (trimmed, lowercase host, trailing slash removed unless the path is meaningful).
- When a pre-approved site matches a request, it bypasses browsing approval workflows.
- Blocked site rules take priority: if a URL matches both a blocked site and a pre-approved site rule, the block applies.
- The global enabled flag and rule list are distributed via endpoint policy API.

5. Download Permission Controls

Decide whether downloads are allowed at all, and what users need to do before one proceeds.

The starting point for download security is a simple question: should users be able to download executable files? When downloads are off, all executables are blocked. When they're on, you can add friction proportional to the risk.

Require approval sends each download request to a portal admin before the user can access or execute the file. Require reason asks the user to justify the download before it proceeds. Both can be enabled together. Applications on your pre-approved download list skip the approval step, so trusted software moves faster while the controls stay in place for everything else.

CONFIGURATION LOCATION
Portal path: Web Access Settings > Authorization > Downloads

CONTROLS

- Allow Downloads toggle
- Require Approval toggle (available when Allow Downloads is ON)
- Require Reason toggle (available when Allow Downloads is ON)
- Save button

BEHAVIOR

- Allow Downloads OFF: all executable downloads are blocked. Require Approval and Require Reason are disabled. The pre-approved downloads list remains active and is the only exception.

- Allow Downloads ON: downloads are permitted subject to any additional controls configured here and elsewhere (MFA, Intune compliance, malware scanning).
- Require Approval ON: each download request must be approved by a portal admin before it proceeds. Downloads matching a rule in the pre-approved downloads list are exempt from this requirement.
- Require Reason ON: the user must provide a reason before initiating a download. An empty reason field rejects the request.
- Require Approval and Require Reason can be enabled independently or together.
- Toggle states are persisted at tenant level and reload from backend on page refresh.

6. Owner-only Download Restriction

On shared devices, restrict downloads to the person the device belongs to.

Shared endpoints create a specific problem: any user who logs in can potentially download software, even if that's not appropriate for their role. Owner-only Download Restriction addresses this by restricting executable downloads to the recognized device owner, as defined in the endpoint inventory.

Other users on the same device can still browse normally if browsing is permitted under your authorization settings. Only the download restriction applies. Ownership is managed centrally in inventory, so adjusting it doesn't require changes to the policy configuration.

CONFIGURATION LOCATION
Portal path: Web Access Settings > Lockdown > Owner

CONTROLS
- Only owner can download: ON/OFF toggle
- Save button

BEHAVIOR
- When ON: only the device owner can download executable files. Any other user logged into the device is blocked from downloading.
- Browsing is not affected by this setting. Any user can browse if browsing is enabled under Authorization.
- The device owner is defined and managed in the endpoint inventory, not on this settings page.
- This is a global setting; it applies across all endpoints in the tenant.
- The saved toggle state is distributed via endpoint policy payload.

DEPENDENCY
Device ownership must be maintained in the inventory for this control to function as expected. If no owner is assigned to a device, behavior should be verified against the endpoint policy specification.

7. MFA-protected Downloads

Require users to verify their identity before a download is released.

For high-risk environments, requiring an approved request isn't always enough. MFA-protected Downloads adds a re-authentication step: before an executable download proceeds, the user must authenticate via SSO using your configured identity provider.

Currently supported through Microsoft 365 and Entra ID, with extensibility for additional providers. When email match is enabled, the authenticated identity must match the email address associated with the endpoint user. If it doesn't, the download is blocked. The combination of approval workflows, MFA, and identity matching means that even if credentials are compromised, a download still can't proceed without a verified authentication event.

CONFIGURATION LOCATION
Portal path: Web Access Settings > Lockdown > MFA

CONTROLS
- MFA required to download: ON/OFF toggle
- Sign-on method dropdown: Microsoft 365 / Entra ID (extensible for additional SSO providers)
- Email match: ON/OFF toggle
- Save button

BEHAVIOR
- MFA required to download OFF: all MFA-related fields are disabled; MFA is not enforced for downloads.
- MFA required to download ON: the user must authenticate via the configured SSO provider before the download is released.
- Sign-on method is required when MFA is ON.
- Email match ON: the identity authenticated during MFA must match the email address associated with the endpoint user. If they do not match, the download is blocked.
- Email match OFF: MFA is required but the authenticated identity does not need to match the endpoint user.
- Configuration is persisted at tenant level and distributed via endpoint policy API.

DEPENDENCY
An Entra ID / Microsoft 365 tenant must be connected for the sign-on method to function.

8. Intune Compliance Gating for Downloads

Stop downloads on devices that don't meet your compliance baseline.

Device compliance and software access should be connected. Intune Compliance Gating for Downloads enforces that connection by blocking executable downloads on any device that isn't marked as compliant in Microsoft Intune, regardless of whether downloads are otherwise permitted.

Browsing is unaffected. The restriction applies at the point of download only, so users on non-compliant devices retain access to the web while the higher-risk action is blocked until the device is brought back into compliance.
This setting requires the Entra ID Connector to be configured.

CONFIGURATION LOCATION
Portal path: Web Access Settings > Lockdown > Intune

CONTROLS
- MFA required to download: ON/OFF toggle
- Sign-on method dropdown: Microsoft 365 / Entra ID (extensible for additional SSO providers)
- Email match: ON/OFF toggle
- Save button

BEHAVIOR
- MFA required to download OFF: all MFA-related fields are disabled; MFA is not enforced for downloads.
- MFA required to download ON: the user must authenticate via the configured SSO provider before the download is released.
- Sign-on method is required when MFA is ON.
- Email match ON: the identity authenticated during MFA must match the email address associated with the endpoint user. If they do not match, the download is blocked.
- Email match OFF: MFA is required but the authenticated identity does not need to match the endpoint user.
- Configuration is persisted at tenant level and distributed via endpoint policy API.

DEPENDENCY
An Entra ID / Microsoft 365 tenant must be connected for the sign-on method to function.

9. Pre-approved Downloads

Stop downloads on devices that don't meet your compliance baseline.

When Require Approval is enabled, pre-approved download rules let known-safe software through without generating a request every time. Rules can be based on source website, direct URL, SHA256 checksum, vendor certificate, or a combination of vendor and application name, so trust can be granted broadly at the publisher level or narrowly at the file level.

Pre-approval only bypasses the manual approval step. MFA, Intune compliance checks, and malware scanning still apply.

CONFIGURATION LOCATION
List page: Web Access Settings > App Control > Pre-approved
Create/Edit page: Web Access Settings > App Control > Pre-approved > New entry / row selection

LIST PAGE CONTROLS
- Enabled: global ON/OFF toggle; when OFF, no pre-approved download rules are evaluated
- Grid columns: Type, URL/Identifier, Log (ON/OFF indicator)
- New entry button: opens the Create page
- Export buttons: PDF, XLSX, CSV

CREATE/EDIT CONTROLS
- Type dropdown: determines which fields are shown
- Dynamic fields (varies by type, see Rule Types below)
- Log to auditlog: ON/OFF toggle per rule
- Internal comments (optional)

RULE TYPES
- Pre-approve downloads from website: Root URL (domain or domain + subpath; scheme not required)
- Pre-approve download URL: Direct URL (full URL or partial path; scheme not required)
- Pre-approve file checksum: Application name + SHA256 checksum (64 hex characters). Browse button available to extract checksum from an uploaded executable.
- Pre-approve vendor (digital certificate): Vendor certificate, collected via Browse.
- Pre-approve vendor and application name: Application name + vendor certificate, collected via Browse.

BEHAVIOR
- The global Enabled toggle must be ON for any pre-approval rule to be evaluated.
- When a download matches a pre-approved rule, it bypasses the Require Approval workflow.
- MFA, Intune compliance checks, and malware scanning are applied regardless of pre-approval status.
- SHA256 values must be exactly 64 hexadecimal characters. Invalid formats prevent saving.
- Browse buttons extract the checksum or certificate from an admin-selected local file; the extracted value is stored by the portal, not the file itself.
- Rules and the global enabled flag are distributed via endpoint policy payload.

10. Blocked Downloads

Hard-deny specific executables, URLs, or publishers regardless of other settings.

Blocked download rules give you a way to stop specific software from ever reaching an endpoint, even when downloads are generally permitted and a matching pre-approved rule exists. Like pre-approved rules, blocks can be defined by source website, direct URL, SHA256 checksum, vendor certificate, or vendor and application name.

Each rule can carry a custom blocking message for users who hit it, and can be flagged for audit logging independently. Hard-deny rules take priority over every other download permission, including pre-approval.

CONFIGURATION LOCATION
List page: Web Access Settings > App Control > Blocked
Create/Edit page: Web Access Settings > App Control > Blocked > New entry / row selection

LIST PAGE CONTROLS
- Enabled: global ON/OFF toggle; when OFF, no blocked download rules are enforced
- Grid columns: Type, URL/Identifier, Log (ON/OFF indicator)
- New entry button: opens the Create page
- Export buttons: PDF, XLSX, CSV

CREATE/EDIT CONTROLS
- Type dropdown: determines which fields are shown
- Dynamic fields (varies by type, see Rule Types below)
- Log to auditlog: ON/OFF toggle per rule
- Blocking message (optional): message shown to the user when a download is blocked
- Internal comments (optional)

RULE TYPES
- Block downloads from website: Root URL (domain or domain + subpath; scheme not required)
- Block download URL: Direct URL (full URL or partial path; scheme not required)
- Block file checksum: Application name + SHA256 checksum (64 hex characters). Browse button available.
- Block vendor (digital certificate): Vendor certificate, collected via Browse.
- Block vendor and application name: Application name + vendor certificate, collected via Browse.

BEHAVIOR
- The global Enabled toggle must be ON for any blocked download rule to be enforced.
- Blocking message is optional; if provided, it is displayed to the end user when the block is triggered.
- SHA256 values must be exactly 64 hexadecimal characters. Invalid formats prevent saving.
- URL inputs are normalized on save (scheme-less, trimmed, lowercase host).
- Rules and the global enabled flag are distributed via endpoint policy payload.

11. Machine Learning Auto-Approval

Approve an application enough times and stop being asked about it.

Approval workflows create repetitive admin work. The same trusted download gets requested, reviewed, and approved over and over, and each round trip costs an admin's attention and a user's time.

Machine Learning Auto-Approval builds your approval list as you go. Set a threshold between 1 and 10, and once a download has been manually approved that many times, future requests for it are approved automatically. You get the benefit of a pre-approval list without having to build one ahead of time.

CONFIGURATION LOCATION
Portal path: Web Access Settings > App Control > Machine Learning

CONTROLS
- Enabled: ON/OFF toggle
- Approvals: slider, 1 to 10
- Save button

BEHAVIOR
- Approvals is the number of times a download must be approved before it is auto-approved in future.
- Example: with Approvals set to 2, once a second user is approved for a given download, all future requests for it are auto-approved.
- Approval counts are visible in the reporting section.

DEPENDENCY
Require approval must be ON under Authorization. With it off, Machine Learning has no effect, and the portal displays a warning on the settings page.

12. AI Auto-Approval

Let trivial requests for well-known software approve themselves.

Most download requests are for software nobody would think twice about. AI Auto-Approval scores downloads and vendors in real time on popularity, reputation, and trends, and approves anything meeting the threshold you set.

Two scores are available independently. App Score rates the individual download; Vendor Score rates the publisher. Setting an App Score threshold of 20 means any request scoring 20 or above is approved automatically. Sample scores across 19.5 million known applications are listed in the portal to help calibrate a threshold you're comfortable with, and scores for your own requests can be viewed by expanding entries in the audit log.

CONFIGURATION LOCATION
Portal path: Web Access Settings > App Control > AI Approval

CONTROLS
- AI App Auto-Approval: Enabled ON/OFF toggle, App Score slider (0-100), Save button
- AI Vendor Auto-Approval: Enabled ON/OFF toggle, Vendor Score slider (0-100), Save button

BEHAVIOR
- Requests scoring at or above the configured threshold are auto-approved in real time.
- App and Vendor scoring are enabled and configured separately.
- A reference table of sample application and vendor scores is available on the settings page.

DEPENDENCY
Require approval must be ON under Authorization. With it off, AI auto-approval has no effect, and the portal displays a warning on the settings page.

13. Malware Detection with OPSWAT MetaDefender

Scan files before they can run, using multiple anti-malware engines.

Executable downloads are a primary malware vector, and approval workflows alone can't catch everything. Web Access Management integrates with OPSWAT MetaDefender to scan files associated with download and execution requests before they're allowed through.

Real-time detection checks the file's checksum against known malware signatures when a download is requested. For files that aren't matched locally, cloud scanning sends the file to MetaDefender for analysis across 37+ engines. Files that are flagged can be quarantined automatically, with the action configurable from the portal.

CONFIGURATION LOCATION
Portal path: Web Access Settings > Malware > Detection

CONTROLS
- Real-time detection: ON/OFF toggle
- Cloud scan unknown files: ON/OFF toggle
- Action dropdown: defines what happens when malware is detected (options include Quarantine)
- Real-time malware alert emails: configurable notification to one or more addresses per detection event
- Save button

BEHAVIOR
- Real-time detection ON: the file checksum is checked against known malware signatures when an execution request is received. Flagged files are blocked before execution.
- Real-time detection OFF: no checksum-based scanning is performed.
- Cloud scan unknown files ON: files that are not matched by local signature data are uploaded to MetaDefender for multi-engine cloud scanning. This provides broader coverage for new or unknown threats.
- Cloud scan unknown files OFF: only local signature matching is used.
- Action determines the disposition of a detected file (for example, Quarantine). Available actions are defined by the endpoint implementation.
- Detection events are logged to the portal under Requests / Detected Malware.
- The saved configuration is included in the endpoint policy payload and applied on the next policy sync.

SCANNING ENGINE
Malware scanning is powered by OPSWAT MetaDefender. Scanning capabilities and signature coverage are determined by the MetaDefender service.

14. Audit Logging and Traceability

Keep a per-rule record of what was blocked, allowed, or approved.

Audit logging is configured on a per-rule basis across pre-approved sites, blocked sites, pre-approved downloads, and blocked downloads. When you turn it on for a rule, every event matching that rule gets recorded, providing a traceable record of browsing decisions, download decisions, approvals, bypasses, and blocks. Each entry captures the action taken, the matching rule, and contextual information about the request.
The toggle controls recording, not enforcement, so turning logging off doesn't change what a rule does, only whether it generates a log entry. Approval and denial events are logged regardless, since they're part of the approval workflow history rather than rule-level auditing.

WHERE AVAILABLE

- Pre-approved Downloads: Log to auditlog toggle per rule
- Blocked Downloads: Log to auditlog toggle per rule
- Pre-approved Sites: Log to auditlog toggle per rule
- Blocked Sites: Log to auditlog toggle per rule

CONTROLS

- Log to auditlog: ON/OFF toggle, configured per individual rule on the Create/Edit page for each supported feature.

BEHAVIOR

- When Log to auditlog is ON for a rule, events matching that rule are recorded.
- Audit log entries capture the action taken, the matching rule, and contextual information about the request.
- The Log to auditlog toggle does not affect enforcement; it controls whether an event is recorded, not whether a rule is applied.
- Log state per rule is visible in the list view for each feature area (Log column).
- Approval-related events (approvals, denials) generate records regardless of the per-rule log toggle, as part of the approval workflow history.

EMAIL NOTIFICATIONS AND ITSM INTEGRATION

- Approval outcome emails: nine configurable templates covering all download and site access outcomes (approved, denied, denied with reason). Custom sender, subject, and body per template with [Tag] variable substitution.
- Admin notification emails: alerts sent to configured addresses when requests are created or malware is detected.
- ITSM integration: download and site access events can be pushed to an external ticketing system or helpdesk address via a parallel email channel.
- Email templates can be overridden per sub-setting, so different populations can receive differently branded or worded outcome emails.

15. Sub-Settings

Apply different policies to different groups, without duplicating configuration.

Sub-settings let you override global policy for specific user or device populations, scoped by Active Directory groups, Entra ID groups, or Organizational Units. Different teams, device types, and locations can operate under their own rules without separate tenants or duplicated configuration.

Global settings stay as the baseline. A sub-setting only changes what it explicitly enables, so most of your configuration lives in one place and only the differences get defined per group. The first matching sub-setting wins per policy section, and rules can be reordered in the portal as priorities shift.

Each sub-settings group defines a scope (which users and/or devices it applies to) and a set of overrides (which policy sections it replaces).

OVERRIDE MODEL
Sub-settings do not replace the entire global configuration. Each of the six sidebar sections (Authorization, Lockdown, Malware, App Control, Site Control, Emails) can be independently enabled or disabled within a sub-setting group. Sections that are enabled in the sub-setting override the corresponding global setting for matched users/devices. Sections left disabled fall through to the global setting.

SCOPE
Each sub-setting group is scoped to a combination of:
- Active Directory security groups (by group name)
- Entra ID / Azure AD groups (requires the Entra ID Connector)
- Organizational Units: by name, root path (e.g. \US\Florida\Sales), or fully distinguished name

Multiple scope types combine with AND logic (user must match the user group condition AND the OU condition). Within a single type, the match is OR (user must be in at least one of the listed groups).

PRIORITY
Sub-settings are evaluated in listed order, top to bottom. The first sub-setting that matches a user/device and has a given section enabled wins for that section. A user/device can match multiple sub-settings, but there is no merging; only the first match per section takes effect. Order is adjustable in the portal by dragging.

CLONE AND COMMENTS
Any sub-setting group can be cloned to create a variant with minor differences. A Comments field stores internal documentation (business purpose, owner, group structure), visible in the list view but with no effect on policy evaluation.

DIAGNOSTIC TOOL
To check which devices qualify for which sub-settings:
Settings > Web Access Sub Settings > [Expand group name] > [Who matches this sub-setting?]

TYPICAL SUB-SETTING SCENARIOS
- Finance team: require approval + MFA for all downloads, stricter browser lockdown
- IT staff: downloads allowed freely, browsing unrestricted, separate pre-approved list
- Kiosk / shared devices: Allow Browsing OFF (pre-approved sites only), Allow Downloads OFF, owner-only restriction applied
- Remote or off-network devices: stricter malware scanning, notification email to a separate SOC address