IP address management best practice

Effective management of IP addresses to ensure secure access to digital content

Introduction

Introduction

By convening publishers, institutions and technologists, SNSI works to help solve the cyber-security challenges that threaten the integrity of the scientific record, scholarly systems and the safety of personal data. In these guidelines, we explore IP address management.

For publishers' information security leaders, customer support teams, librarians, and institutional CISOs or IT security teams, robust IP address management is key to maintaining the right balance between accessibility, security, and compliance with licensing agreements. Effective IP Address Management (IPAM) not only safeguards digital content such as journals, articles, and eBooks, but also ensures controlled and secure access for authorized users.

We all play a critical part in ensuring the integrity of IP-based authentication and maintaining access for authorized users. This document outlines the key best practices for managing IP addresses effectively and mitigating common challenges, including audit reviews, geo-blocking, IP allow lists, and dealing with unauthorized access. Our overwhelming purpose in creating this document, though, was to respond to requests from librarians for help and support in their conversations with campus network security colleagues.

These guidelines provide practical guidance on how to ensure only approved institutional IP addresses are granted access to subscription-based content.

Visit www.snsi.info for more information.

Contents

- **Audit at renewals review:** Auditing IP lists as institutional networks evolve.
- **Geo-blocking**: Ensuring compliance with regional access policies.
- **IP allow list:** Ensuring only approved institutional IP addresses are granted access to subscription-based content.
- **Limitation on IP addresses and alerting mechanism:** Setting caps on the number of IP addresses an institution can register.
- **Designation of primary and secondary IPs with limitations:** Helping manage large multi-campus institutions with more granular access.
- **Managing unauthorized access:** Rate limiting and deactivating accounts where necessary.
- **Using third-party tools for IP address management and Security:** Verifying, monitoring, and securing IPs.
- **For Institutional CISOs/Institutional IT Security Teams:** Strengthening IP Address Hygiene and Security

Audit at renewals review

Auditing IP lists as institutional networks evolve

Audit at renewals review

1. **For publisher information security leadership**:

Manual audits are essential for ensuring that only legitimate IP addresses are authorized for access. Institutional networks evolve frequently, with changes to service providers or infrastructure, leading to shifts in IP allocations. Failing to audit these IP lists can expose the system to risks such as unauthorized access or legitimate users being locked out.

Best practices:

- Conduct Regular Audits: Schedule annual or bi-annual reviews to verify that all registered IP addresses are still valid. This reduces risks from outdated or inaccurate IP data.

- Automation: Implement automated tools or workflows to streamline the review and update process across multiple institutions.

2. **For customer support:**

Frequent issues arise from outdated or incorrect IP addresses leading to access denial. Support teams often serve as the first line of defense in identifying and solving access issues.

Audit at renewals review / 2

Best practices:

- Support Communication: When access issues arise, have clear communication channels with institutional IT staff and library administrators to request updated IP address information quickly.
- Proactive Alerts: Notify institutions well in advance of subscription renewals to encourage them to review and update their IP lists.

3. For librarians:

As the key administrators of IP access, librarians can help ensure that IP addresses are up-to-date and correctly registered. Incorrect IPs can cause disruptions in content access, leading to frustration for both students and faculty.

Best practices:

- Regular IP Reviews: Coordinate with your institution’s IT team to regularly review the list of registered IPs and ensure they reflect your current network configuration.
- Institutional Communication: Help maintain open lines of communication with your publishers and internal IT team regarding changes to the institution’s IP Addresses.

Geo-blocking

Ensuring compliance with regional access policies

Geo-blocking

1. For publisher information security leadership::

Geo-blocking is a technique/tool used to ensure compliance with regional access policies. Ensuring that access is geographically restricted to authorized regions helps align with licensing agreements and prevent misuse.

Best practices:

- Implement Geolocation Tools: Integrate IP geolocation services that monitor the geographic origin of access requests to detect and block unauthorized access from outside approved regions.
- Monitor Access Logs: Set up alerts for any access anomalies indicating potential abuse, such as logins from regions outside of authorized geographic zones.

2. For customer support:

Geo-blocking related issues can lead to frustrated users, especially when they are unaware that access restrictions are based on geographic location.

Geo-blocking / 2

Best Practices:

- Clear Communication: When geo-blocking leads to access issues, help clearly explain to users why they are blocked and guide them toward legitimate access methods, such as institutional VPNs.
- Review Compliance Cases: Coordinate with the compliance team so that geo-blocking rules align with institutional agreements.

3. For Librarians:

Understanding geo-blocking helps ensure awareness of which users should or should not have access based on geographic restrictions.

Best Practices:

- Ensure Regional Compliance: Working with publishers to understand any regional restrictions in agreements and ensure that access rights align with the institution’s needs.
- Notify Users: If certain resources are unavailable due to geo-blocking, notify users in advance and provide guidance on alternative methods for accessing content.

IP allow list

Ensuring only approved institutional IP addresses are granted access to subscription-based content

IP allow list

1. For publisher information security leadership:

An IP “allow list” ensures that only approved institutional IP addresses are granted access to subscription-based content. Maintaining control over this list helps mitigate unauthorized access risks.

Best practices:

- Centralize IP Management: Use a centralized platform to manage and review all allowed IPs across subscribed institution(s). This simplifies the process and reduces errors.
- Verification Process: Require two-factor verification or internal approvals for adding new IP addresses to the allow/pre-validated list to prevent accidental or malicious changes.

2. For customer support:

Customer support plays a key role in verifying and updating allowed/pre-validated IP addresses on behalf of institutions, especially when access issues occur.

IP allow list / 2

Best practices:

- Efficient IP Registration: Set up a streamlined, secure process for institutions to submit their IP address lists. This ensures timely updates and accurate data entry.
- Regular IP Updates: Proactively contact institutions that may have stale or outdated IPs, ensuring that their access is not interrupted.

3. For librarians:

To maintain seamless access for library users, librarians may want to collaborate with the publishers as needed to ensure that IP addresses registered are correct and up to date.

Best practices:

- Self-Management Tools: Librarians can request self-service portals from publishers to easily update IP addresses in real time.
- Monitor Changes: Review IP lists periodically, especially when there are changes to the institution’s network infrastructure.

Limitation on IP addresses and alerting mechanism

Setting caps on the number of IP addresses an institution can register

Limitation on IP addresses and alerting mechanism

1. For publisher information security leadership:

Setting caps on the number of IP addresses an institution can register helps maintain security and prevent excessive or unauthorized access. Alarms should be triggered when these limits are exceeded, signaling potential abuse or mismanagement.

Best practices:

- Set Thresholds: Establish reasonable caps for the number of IP addresses based on institutional size and usage patterns. Ensure automated alarms notify the appropriate staff when limits are breached.

- Review IP Requests: Requests to exceed the cap should be manually reviewed to confirm that they are justified.

2. For customer support:

Anomalies in the number of registered IP addresses often lead to support issues related to unauthorized access or incorrect data entry.

Limitation on IP addresses and alerting mechanism / 2

Best practices:

- IP Caps and Escalation Protocol: Work closely with publisher CISOs to establish protocols for escalating cases where an institution’s registered IPs exceed the normal cap.
- Log and Track IP Requests: Use tools to log all IP changes, particularly when institutions request to exceed their IP cap. This helps identify potential misuse early on.

3. For librarians:

Be aware of the limitations on the number of IPs the institution can register and work within those constraints to ensure optimal access.

Best practices:

- Coordinate with IT: Work closely with your IT department to ensure that registered IPs reflect the actual needs of your institution, and that obsolete or redundant IPs are not registered.
- Monitor Cap Usage: Track the institution’s IP usage to align with what has been agreed in the applicable license. If additional IPs are needed, contact the publisher.

Designation of primary and secondary IPs with limitations

Helping manage large multi-campus institutions with more granular access

Designation of primary and secondary IPs with limitations

1. For publisher information security leadership:

Differentiating between primary and secondary IP addresses helps manage large, multi-campus institutions where access needs to be more granular. Setting caps on secondary IPs ensures only appropriate networks are accessing content.

Best practices:

- Categorize IPs: Identify and categorize the institution’s primary IP addresses (main campus) and secondary IP addresses (satellite campuses, research centers).
- Limit Secondary IPs: Set caps on secondary IPs and regularly review their usage to avoid unnecessary or outdated IP addresses from remaining on the allow list.

2. For customer support:

Understanding the difference between primary and secondary IPs can help in resolving access issues and responding to institutions more effectively.

Designation of primary and secondary IPs with limitations / 2

Best practices:

- Monitor IP Categories: Provide institutions with a clear system for categorizing primary and secondary IPs and help them manage this distinction effectively.

- Alerts for Overuse: Set up alerts for any spikes in secondary IP registrations that exceed the agreed-upon cap.

3. For librarians:

Ensure that the primary and secondary IP addresses registered accurately reflect the institution’s usage needs and align with what has been agreed in the license.

Best practices:

- Limit IP Registrations: To avoid access issues caused by unnecessary, outdated, or unused secondary IPs - only register secondary IPs when needed and remove outdated or unused IPs.

- Cap Increases: If the institution needs to exceed what has been agreed in the license, contact the publisher to explain the reason, e.g., campus size or infrastructure changes.

Managing unauthorized access

Rate limiting and deactivating accounts where necessary

Managing unauthorized access

1. For publisher information security leadership:

Unauthorized access can occur through IP spoofing, over-registration of IPs, or credential sharing. Organizations can limit the number of requests or data that can be transmitted within a specific timeframe. Unauthorized access often leads to support tickets when institutions are locked out of their accounts or restricted in their data transmission rates. Ensure clear procedures are in place for handling these scenarios.

Best practices:

- Request/Data Limiting Mechanisms: Limit the number of downloads per IP address or account within a given time frame. This helps reduce the potential impact of unauthorized access.

- Account Disabling: If misuse is detected, quickly disable access for the affected IP range or account while investigating further. This helps protect against theft of licensed content as well as other important institutional data.

2. For customer support:

Unauthorized access often leads to support tickets when institutions find themselves locked out or having the number of requests or data that can be transmitted within a specific timeframe limited. Ensure clear procedures are in place for handling these scenarios.

Managing unauthorized access / 2

Best practices:

- Communicate Clearly: When request and/or data limiting, or account disability occurs, explain the reason to institutions clearly, offering guidance on how to restore access once the issue is resolved.

- Report Suspicious Activity: Coordinate with the compliance and security teams to report unauthorized access and respond quickly to prevent further misuse.

3. For librarians:

Unauthorized access can result in lockouts and sometimes happens through credential sharing or overuse of IP addresses. Avoid these issues through education and periodic audits.

Best practices:

- Encourage Responsible Use: Educate users about the importance of adhering to licensing agreements.

- Secure Credentials and IP Ranges: Implement robust access controls to ensure that institutional login credentials and approved IP ranges are accessible only to authorized users and conduct regular audits to ensure compliance with licensing agreements.

Using third-party tools for IP address management and security

Verifying, monitoring, and securing IPs

The mention of specific tools or services in this document is for informational purposes only and does not constitute an endorsement or recommendation of any vendor or product. Institutions should evaluate and select security tools based on their specific requirements, risk assessments, and internal policies.

Using third-party tools for IP address management and security

When managing IP addresses for academic publishing access, third-party tools play a crucial role in verifying, monitoring, and securing IP ranges. These tools provide essential insights into ownership, location, reputation, and potential security threats, which are critical for ensuring that only authorized users from legitimate institutions access content.

Here’s an overview of some classes of tools that can enhance IP address management:

IP lookup and ownership verification tools

- Tools like WHOIS (IPWHOIS.io) and IPinfo allow users to check the ownership, registration details, and geographic location of IP addresses. These services help ensure that the IP addresses registered by institutions are accurate and properly linked to authorized networks. Users of these tools can verify that the IP address range belongs to the expected institution, reducing the risk of unauthorized access, data theft, and lockouts.

Using third-party tools for IP address management and security / 2

Security and reputation monitoring tools

Tools like VirusTotal and Talos Intelligence are critical for checking whether any registered IPs are associated with malicious activities, such as malware distribution, spam, or botnets. These tools aggregate data from multiple security sources to provide a reputation score for IP addresses, helping identify compromised or suspicious IPs that could pose a security threat. Regular monitoring of IP reputations ensures that access isn't unknowingly allowed to users from networks that are at high risk of being involved in cyber threats.

Geolocation and routing tools

IP2Location and bgp.he.net (Hurricane Electric BGP Toolkit) are useful for confirming the geographical location and routing information of IP addresses. This helps ensure alignment with geo-restrictions where appropriate. These tools also help track how traffic is routed across the internet, identifying potential misconfigurations that could result in unauthorized access.

Using third-party tools for IP address management and security / 3

Fraud detection and Proxy identification tools

Tools like IPQualityScore are designed to detect fraudulent activities, proxies, VPNs, and other attempts to mask true user identities. Since some users may attempt to use proxies or VPNs to bypass institutional restrictions, these tools can be used to identify suspicious IP addresses or traffic patterns, preventing abuse and ensuring that access is limited to legitimate users.

Best practices for using third-party tools

1. Integrate into automated systems: Where possible, integrate tools for IP address management and security into automated workflows that flag suspicious IP addresses, outdated registrations, or unusual activity. Automating checks on IP reputation, geolocation, and ownership helps maintain secure access without overwhelming IT or support teams.

2. Audit and review: Perform regular audits of institutional IP addresses using tools that provide ownership, reputation, and geographic insights. This ensures that registered IPs remain accurate and align with agreed-upon licenses.

Using third-party tools for IP address management and security / 4

3. Combine tools: No single tool covers all aspects of IP address management, so it's important to combine several tools to get a comprehensive view of the institution's network. For instance, an IP that passes a WHOIS check might still be flagged for reputation issues by VirusTotal or show up as a proxy on IPQualityScore.

4. Be proactive in response: Set up alerts and response mechanisms for when these tools flag suspicious or anomalous activity. IP ranges associated with negative reputation or proxies should be reviewed and, if necessary, blocked or subjected to further scrutiny before access is granted.

Not Limited to These Tools

While the tools mentioned — WHOIS (IPWHOIS.io), IPinfo, VirusTotal, Talos Intelligence, IP2Location, DNSstuff, bgp.he.net, and IPQualityScore—are worth evaluating for possible use for an institution's IP address management, they are by no means the only solutions available. Publishers and Librarians should explore other tools and services that may better meet their specific needs, industry standards, or integration requirements. Ultimately, a combination of several tools and best practices will provide the most effective approach to IP address management and security in academic publishing.

For Institutional CISOs/ Institutional IT Security Teams

Strengthening IP Address Hygiene and Security

For Institutional CISOs/ Institutional IT Security Teams

Institutional CISOs/Institutional IT Security Teams can play a critical role in upholding the integrity of IP-based authentication by ensuring that only accurate and authorized IP addresses are submitted to publishers.

As custodians of the institution's network perimeter, Institutional CISOs/Institutional Security Teams are uniquely positioned to prevent misuse, reduce administrative overhead, and improve collaboration with publishers by implementing sound IP address management practices.

While librarians and access administrators often manage the operational aspects of IP registration, the institutional security team can support them by ensuring the underlying infrastructure is well maintained, accurately documented, and protected from abuse.

Best practices:

- Maintain Authoritative IP Inventory: Ensure the institution maintains a centralized and regularly updated record of all externally routable IP ranges eligible for publisher registration. Implement governance workflows to ensure all IPs submitted for publisher access are subject to internal validation. Require sign-off from relevant IT or security personnel before changes are communicated externally.

For Institutional CISOs/ Institutional IT Security Teams / 2

- Limit to Static, Controlled IP Ranges: Only submit IP ranges that are static, institution-owned, and allocated for academic or administrative use. Exclude dynamic, transient, or personally assigned IPs, including those used for VPNs or remote access, which may introduce risk of abuse or breach of licensing terms.

- Support IP Classification: Work with internal stakeholders to differentiate between primary IPs (e.g. central library systems, campus proxies) and secondary IPs (e.g., satellite sites, temporary research networks). Apply internal controls to manage these designations and review their relevance periodically.

- Support Monitoring of Network Usage Patterns: Consider integrating monitoring capabilities that help detect unusual outbound activity from institutional IPs to publisher platforms. Sudden surges in traffic or anomalous usage may indicate automated tools or misuse, and early detection can reduce the risk of lockouts or IP/account restrictions.

- Respond Promptly to Abuse Notifications: Treat reports from publishers regarding suspicious activity from institutional IPs as formal incident inputs. Designate a technical contact within the security or networking team to investigate, coordinate with affected stakeholders, and provide feedback to the publisher.

For Institutional CISOs/ Institutional IT Security Teams / 3

- Align with Regional Access Controls: Ensure the institution’s IP traffic is routed in a way that aligns with licensing-based geographic restrictions. Avoid misconfigured networks or anonymized routing that could cause users to appear out-of-region and risk access disruption.

- Support Periodic Review and Security Posture Checks: Where practical, support periodic reviews of registered IP ranges to verify they remain assigned to the institution, are free from signs of misuse, and comply with both internal security policies and publisher licensing or acceptable-use requirements. Integrating these checks into your regular network-monitoring or intelligence processes helps maintain alignment with institutional standards and ensures secure, policy-compliant access to content.

Doing more:
We want to hear from you

Part of SNSI's objective is to be a strong partner for our communities. As we move forward together, questions we are asking ourselves include:

- What support do librarians need from publishers and technology providers to better manage and navigate the need for access with the need for security and data protection?
- How can we work with IT security within institutions to design systems that meet both researcher and organisational goals to help people prioritize safety over convenience?
- What support do institutions need to implement and uphold a secure network system to safeguard users and ensure streamlined simple access?
- What more can publishers do to make their platforms easy to access?
- How can we better work together to address challenges of balancing security and simple authentication methods from multiple locations and devices?
- Is more internal education and training needed around the wider threats of cyber and data breach?

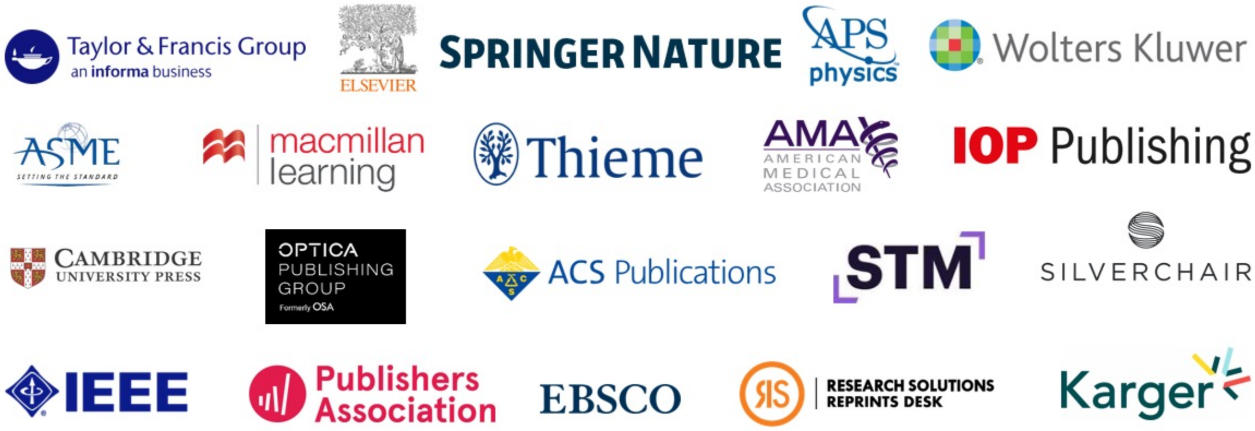
We want to hear from you!

Contact us via the website **www.snsi.info**

About SNSI

- SNSI brings together publishers and institutions to solve cyber-challenges threatening the integrity of the scientific record, scholarly systems and the safety of institutional and personal data.
- Members include large and small publishers, learned societies and university presses and others involved in scholarly communications.

Participating organisations


Taylor & Francis Group an informa business
ELSEVIER
SPRINGER NATURE
APS physics
Wolters Kluwer
ASME SETTING THE STANDARD
macmillan learning
Thieme
AMA AMERICAN MEDICAL ASSOCIATION
IOP Publishing
CAMBRIDGE UNIVERSITY PRESS
OPTICA PUBLISHING GROUP Formerly OSA
ACS Publications
STM
SILVERCHAIR
IEEE
Publishers Association
EBSCO
RESEARCH SOLUTIONS REPRINTS DESK
Karger

For more information,
please visit
www.snsi.info