Blumira

NIST Compliance Reports

COMPLIANCE IS EASY WITH BLUMIRA'S REPORTS

Pre-built reports sent straight to your inbox to prove your NIST compliance to an auditor.

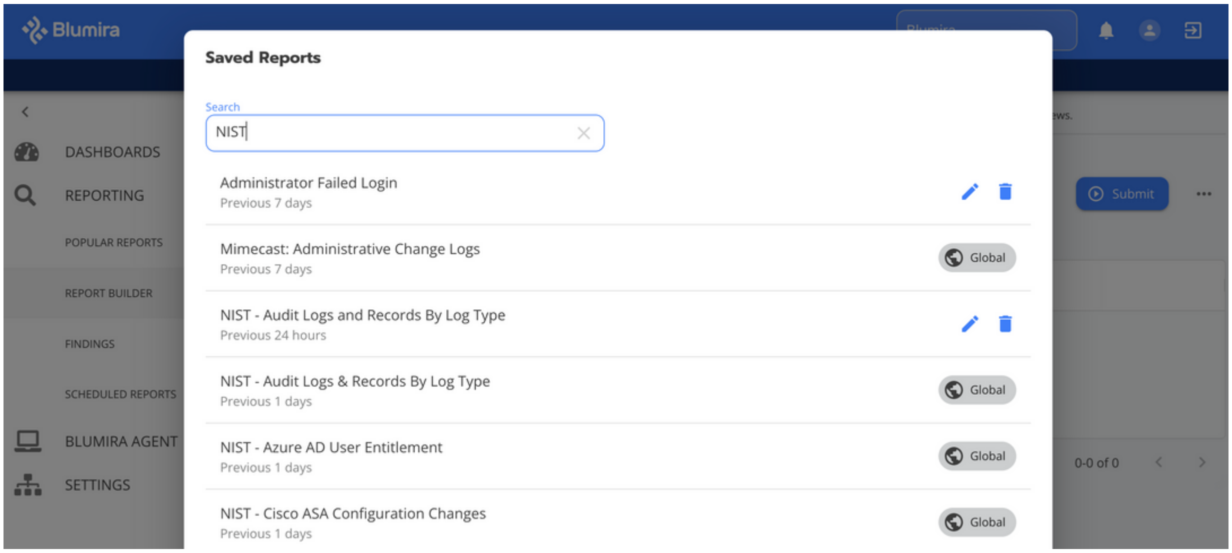
Any organization seeking to meet NIST compliance requirements needs to show proof of their compliance. **Blumira's SIEM quickly and easily provides the reports you need for certain NIST controls.**

These pre-built reports can be searched, run, and scheduled to send to your inbox regularly. That way, when you need to prove your compliance to an auditor, you can easily hand over Blumira's time/date-stamped reports.

NIST 800-171 Controls	Blumira Report
NIST 3.1 Access Control 3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	**(NIST) Unauthorized Access Attempts** Blumira's report lists out all failed login attempts, access denied events, etc. over the last 90 days. This verifies proper logging and monitoring of access. **Available for:** Windows & Linux
3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute	**(NIST) Service Account Access** This report lists all service account login events to help you confirm appropriate use of these accounts. **Available for:** Azure & Windows
3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.	**(NIST) User Entitlement** This report shows all user permissions and roles to validate proper access controls and least privilege. **Available for:** Azure AD, GSuite (Now Google Workspace) & Windows
3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	**(NIST) Privilege Elevations** Blumira's report shows all instances where user privileges were temporarily escalated, such as sudo commands. This verifies proper approval and monitoring. **Available for:** Windows & Linux
3.1.12 Monitor and control remote access sessions	**(NIST) VPN Connection** This lists all VPN connection events for remote users within your environment. This validates connections were authorized. **Available for:** Fortigate, GlobalProtect, Cisco ASA, SonicWall, Sophos, & WatchGuard

NIST 800-171 Controls	Blumira Report
NIST 3.3 Audit & Accountability 3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	**(NIST) Audit Logs & Records** This report shows your "earliest" log by type to help you prove data retention and show length of time period.
NIST 3.4 Configuration Management 3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.	**(NIST) Configuration Changes** Blumira's report lists all configuration changes made to systems and devices over the last 90 days, such as firewall changes. This verifies proper change management. **Available for**: Cisco ASA, Fortigate, & Palo Alto
NIST 3.14 System & Information Integrity 3.14.2 Provide protection from malicious code at designated locations within organizational systems.	**(NIST) Malware Detection** This report lists out instances where anti-malware tools detected malware over a certain time period. **Available for**: Microsoft 365, Carbon Black, CrowdStrike, Cylance, Defender

This feature is available to all paid Blumira customers and can be found by navigating to **Reporting** > **Report Builder**, clicking Load Saved Report and typing “NIST” into the search box.



Saved Reports

Search: NIST

Administrator Failed Login Previous 7 days	
Mimecast: Administrative Change Logs Previous 7 days	Global
NIST - Audit Logs and Records By Log Type Previous 24 hours	
NIST - Audit Logs & Records By Log Type Previous 1 days	Global
NIST - Azure AD User Entitlement Previous 1 days	Global
NIST - Cisco ASA Configuration Changes Previous 1 days	Global

> We’re required by CJIS and IRS Pub 1075 compliance to review our logs daily. **Blumira has saved us time** because we can’t monitor all of our logs — we would need a team of 100 to go through all of these logs manually.
>
> Mike Morrow
> Technical Infrastructure Manager
> Ottawa County

Ottawa County

TRY XDR TODAY

Blumira makes security easy and effective for SMBs, helping them detect and respond to cybersecurity threats faster to stop breaches and ransomware.

Contact us to try Blumira’s SIEM + XDR platform:

- SIEM deployment in minutes
- Managed detection rules
- Endpoint visibility and response
- Automated response

Visit blumira.com/trial