Auvik Networks System Security

www.auvik.com

CONTENTS

YOU CAN'T TAKE CHANCES WITH AN IT NETWORK.

Security is a big part of network management today. Are the infrastructure and data you manage safe? As a network administrator or managed service provider, you carry a lot of responsibility. We know that.

It's why we built our network management system from the ground up with safeguards in mind. Our goal is always to make your life easier. Less stressful. More effective.

This white paper will give you an overview of how Auvik collects and transfers data, and the security protocols we follow to keep the networks you manage safe.

Read on to learn more.

WHAT IS AUVIK?

Auvik is a cloud-based system that provides unprecedented insight into networks and automates complex and time-consuming tasks. Auvik keeps network maps and documentation up to date in real-time, captures and manages device configurations, monitors network performance, alerts you to potential network issues, and more.

Data security was built into Auvik from the beginning. We've followed industry best practices to ensure Auvik is as safe and secure as the most well-known and respected cloud-based offerings.

WHAT IS THE COLLECTOR AND WHAT DOES IT DO?

Using Auvik begins with installing the Auvik collector on a network.

The collector is a piece of code that uses a number of protocols to gather information about the network, such as topology details, configurations, and network statistics. The collector summarizes and sends that information to the Auvik servers over encrypted connections.

When you deploy the Auvik collector to a network, it's uniquely configured to be associated *only* with the account that created it. There's no way another Auvik customer account can communicate with a collector you're using, either accidentally or purposefully.

The collector only establishes outbound connections; our cloud servers cannot establish an inbound connection.

HOW IS THE AUVIK COLLECTOR SECURED?

The collector sends information to the Auvik servers using a TLS-encrypted (minimum TLSv1.2) web socket that follows industry standards for secure data transmission on the internet. The collector uses certificate authentication to ensure it's communicating with the Auvik servers.

Vulnerability management and patching

Auvik tests the collector code for security vulnerabilities before release.

All patches to the collector code go through a quality assurance process before being scheduled for deployment. Critical and high vulnerabilities are released as hotfixes outside of the regular deployment schedule.

The collector supports multiple installation methods, as detailed in **the Auvik Knowledge Base**. On the Windows service, operating system updates and patches are handled by the policy on the underlying OS. For the OVA or scripted appliance methods, the Auvik collector is configured to conduct a daily check for updates to all installed packages. The collector is also configured to update the packages nightly if an update is available.

WHAT COMMUNICATION PROTOCOLS DOES AUVIK USE?

Auvik uses these communication protocols to communicate with networks and cloud-based sources of network data:

- **HTTP(S)**
  Hyper Text Transfer Protocol (Secure)
- **ICMP**
  Internet Control Message Protocol
- **mDNS**
  multicast Domain Name System
- **NetFlow**
- **SMB**
  Server Message Block
- **SNMP**
  Simple Network Management Protocol
- **SSH**
  Secure Shell
- **Syslog**
- **Telnet***
- **TFTP**
  Trivial File Transfer Protocol
- **UPnP**
  Universal Plug and Play
- **WS-Management**
  Web services management

** Telnet is used only when SSH is not available or when a user has specified its use.*

The collector sends information to the Auvik servers through an TLS-encrypted web socket, following industry standards for secure data transmission on the internet. The collector uses certificate authentication to ensure it's communicating with the Auvik servers.

HTTPS
HTTPS is the secure protocol over which data is sent between your browser and the Auvik servers. It's the transport mechanism for protocols such as WS-Management APIs, VMware vSphere APIs, Meraki cloud dashboard APIs, and others.

ICMP
ICMP is one of the main protocols of the Internet Protocol Suite. It's most often used by network devices, like routers, to send error messages. It can also be used to relay query messages. Auvik uses ICMP to ping devices on a network.

mDNS
mDNS resolves host names to IP addresses. It works by sending an IP multicast query message that asks the host having that name to identify itself.

NetFlow
NetFlow and similar protocols such as IPFIX and J-Flow are designed to collect metadata about Internet Protocol (IP) connections, including source and destination IP and ports.

SMB
SMB is an application-layer network protocol that Auvik uses to discover printers, serial ports, and miscellaneous communications between network nodes.

SNMP
SNMP is an internet-standard protocol for collecting and organizing information about devices on an IP network.

SSH
Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers. Auvik uses SSH to remotely log in to network devices and scrape the results of configuration commands as a way of getting device configuration and status information.

Syslog
Syslog is a well-known protocol for event notifications across networks. The versatility of the protocol makes syslog a de facto standard for the monitoring and troubleshooting of almost any device or service. Auvik ingests syslog over UDP.

Telnet
Telnet is a client-server protocol historically used to send clear text across a network. Today, most administrators prefer SSH, which provides much of the same functionality as Telnet but with the addition of encryption and public key authentication. Auvik will only use Telnet to communicate with your network if SSH is not available or if you've specified its use.

TFTP
TFTP is a simple file transfer protocol that Auvik uses to send a configuration file to the network when you request a configuration restore. It's also used to back up some device configurations.

UPnP
UPnP is a set of networking protocols that allows devices to discover each other's presence on a network.

WS-Management
WS-Management is an open standard defining a SOAP-based protocol for the management of servers, devices, applications and various web services. WS-Management provides a common way for systems to access and exchange management information across IT infrastructure.

Source: Wikipedia

WHAT INFORMATION DOES AUVIK COLLECT AND HOW IS IT HANDLED?

1) Auvik collects the authentication credentials of network devices.

Auvik needs credential information to see devices and how they're connected to one another. All the credentials shared with Auvik are sent to the cloud and stored there using **AES-256** encryption. They're decrypted and made available to the system only as needed for delivering product features.

AES-256

The Advanced Encryption Standard or AES is a symmetric block cipher used by the US government to protect classified information. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. AES-256 encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 256-bits.

Source: TechTarget

2) Auvik logs the configuration data of network devices.

Auvik requires configuration data to better understand a network. Auvik analyzes how configuration changes affect performance, allowing you to optimize network performance over time. Like credentials, all configuration data is encrypted using AES-256.

3) Auvik collects anonymized network metadata.

Auvik usually keeps some high-level anonymized metadata from every account. For example, we might log the connection speeds between devices, the number of bytes sent, and usage statistics. We aggregate this metadata with metadata from other accounts. It's used solely for the purpose of analyzing and optimizing our system performance. The data isn't encrypted but is stored in a secure database. Since the data is anonymized, no one could ever acquire information about a specific network with it.

A feature called Auvik TrafficInsights™ allows you to troubleshoot network performance problems by collecting metadata about traffic flowing through the network. This metadata includes source address, source port, destination address, destination port, and amount of data transferred.

Auvik *doesn't* see any traffic content sent through a network.

If someone sends an email on your network, for example, Auvik would know how many bytes were transmitted. But there's no way for our system to read the content of the transmitted packets.

HOW DOES AUVIK USE NETWORK INFORMATION?

Auvik uses the information gathered by the collector to deliver product features. For example, the information is used to draw a network map, create device profiles for inventory, and log device configurations.

Auvik analyzes, distills, and visually renders network information, then shows it to your approved users through a secure login from a web browser.

HOW IS NETWORK INFORMATION KEPT SAFE ON AUVIK SERVERS?

Like many SaaS offerings, Auvik stores data in a cloud-hosted, multi-account environment. We follow industry best practices in every aspect of secure data collection and storage.

Auvik servers use an industry standard four-tier architecture, with security protocols at every layer. Even if someone gained unauthorized access to our system, the risk of them being able to compromise all four layers to see or make use of customer data is extremely low.

As soon as information from a network reaches the Auvik system, it's partitioned in such a way that it's impossible for data to cross from one account to another.

At Auvik, we make it impossible for non-approved employees to access customer information. Systems holding customer data are not exposed publicly and can only be accessed by authorized personnel through a controlled access mechanism. As well, we regularly rotate credentials based on industry best practices.

HOW IS USER ACCESS TO AUVIK CONTROLLED?

An Auvik account allows for multiple users. Each user has their own login credentials. The account administrator(s) can specify whether users should have full access to view and change things on the network or read-only access. Users with permissions to define other users' roles can further specify which client networks each user has access to.

Role-based access controls

Auvik offers granular role-based access controls. Each user is designated a specific role on each client account. As a starting point, Auvik offers seven preset roles. You can tailor each of these presets, as well as add custom roles you build yourself.

Auvik Application Programming Interface (API) access

Auvik exposes a set of APIs for customers and third-party integrators to tap into. Data accessed through the API is requested through a specified username and bearer token and is scoped to the set of client networks the user has access to.

For system-driven integrations, Auvik also provides the ability to create an API-only user that revokes the ability to access any data through the Auvik interface other than the user's profile information.

Bearer tokens can be (re)generated or revoked from within a user's profile.

Auvik support access

Auvik support team members usually need at least read-only access to your account to investigate and troubleshoot issues. You can grant the Auvik support group one of three access levels:

1) Read-only
2) Admin (read/write)
3) No access

These access levels can be set globally (across all clients) or per client. The default access level is read-only.

Single sign-on

Auvik provides single sign-on capabilities through two industry standards:

1) SAML 2.0
2) OAuth 2.0

SAML integration with an identity provider like Microsoft's Azure Active Directory enables you to manage authentication from a central location and to use more advanced policies through your identity provider. You can choose who has to use SAML authentication.

If SAML authentication isn't enforced, users can enable single sign-on with the OAuth protocol through Google's G Suite or Microsoft's Azure Active Directory. This can be set up after receiving their initial invitation to Auvik or later through their user profile.

Two-factor authentication

For additional security, Auvik requires two-factor authentication for all users that don't use single sign-on. Auvik two-factor authentication uses the time-based one-time password (TOTP) algorithm. TOTP ensures compatibility with mobile apps like Microsoft Authenticator, Authy, and Google Authenticator.

WHERE IS DATA STORED?

Auvik is hosted on Amazon Web Services (AWS) in several geographies, including Ireland, Germany, Australia, Canada, and multiple regions in the United States. Your data will be stored in the best region for your location. If your Auvik account is through an Auvik channel partner, the location of your data may be aligned to the channel partner's location.

HOW IS THE DATA CENTER SECURED?

Physical security

Auvik is hosted on Amazon Web Services (AWS). Amazon's physical and operational security processes are documented in **Amazon Web Services: Overview of Security Processes**, which outlines AWS data center controls such as:

- Physical and environmental security
- Fire detection and suppression
- Power
- Climate and temperature
- Storage device decommissioning
  - AWS uses the techniques detailed in NIST 800-88 (*"Guidelines for Media Sanitization"*) as part of the decommissioning process.
- Amazon's fault-tolerant infrastructure design
  - Core applications are deployed in an N+1 configuration so that in the event of a data center failure, there's sufficient capacity for traffic to be load-balanced to the remaining sites.
- Certification
  - AWS holds numerous security certifications, which can be reviewed at **https://aws.amazon.com/compliance/**.

Security monitoring

Auvik monitors its production environment through a variety of means including log aggregation and monitoring, intrusion detection, and daily audits of the platform to ensure a strong security posture and a proactive approach to potential threats.

Application security

Auvik's software is developed and tested following the principles set out in the Open Web Application Security Project (OWASP) Top Ten framework to help ensure no vulnerabilities are deployed into production.

Vulnerability management and patching

Auvik tests all code for security vulnerabilities before release, and regularly scans its network and systems for vulnerabilities.

Patches go through a quality assurance process before being scheduled for deployment. Critical and high vulnerabilities are released as hot fixes outside of the regular deployment schedule.

We use a third party to conduct annual vulnerability scans and penetration tests against Auvik's software.

Endpoint protection

Auvik deploys anti-virus software on all employee laptops and desktops and manages the software centrally to make sure all signatures are up to date. Auvik also performs daily vulnerability scanning and patching from a centralized management platform within our IT organization. With centralized reporting, we can make sure security incidents are properly quarantined and escalated for further action where needed.

Incident management

Auvik has a defined process for managing security and privacy incidents. The process can be initiated by an Auvik customer, internal employee, or the public. If a security incident is identified, we follow this high-level process:

- The security or privacy incident is identified and communicated to the Security Incident Response Team (SIRT).
- We assess the incident to determine its severity, priority, scope, and impact.
- We make recommendations for containing, eradicating, or recovering from the incident, then execute on the recommendations.
- Where applicable, we scan the environment(s) to make sure we've completely mitigated the incident.
- We communicate with internal resource teams, stakeholders, and Auvik customers based on the findings of triage and analysis.
- We gather feedback and look at lessons learned to evolve our incident response process and procedures. Where applicable, we identify and log the incident's root cause.

Vendors and subcontractors

Auvik reviews all relevant vendors and subcontractors to make sure they also provide an appropriate level of security.

Security awareness

Auvik has a security awareness program to ensure all employees understand the importance of security and how it intertwines with their workday.

New employees are required to take security training, and throughout the year we perform audits to make sure training is completed. We also have regular refresher training for all staff once per quarter to ensure security is top of mind for everyone at Auvik.

Auvik uses several intelligence sources to keep up to speed on the latest security threats. This information is shared regularly with staff to make sure everyone is aware of threats and knows what to do if they encounter them.

WHAT PRIVACY REGULATIONS DOES AUVIK COMPLY WITH?

GDPR

The General Data Protection Regulation (GDPR) is a set of data governance laws that went into effect within the European Union on May 25, 2018. Organizations outside the EU are also affected, since any organization that works with the personal data of EU residents now has obligations to protect the data.

Auvik has a privacy policy in place that takes GDPR principles into account. We also understand our obligation as a data controller to support our partners in their GDPR compliance.

WHAT IS AUVIK'S DATA RETENTION POLICY?

If you ever decide to cancel your Auvik subscription—which you may do at any time—the network data in your account is completely recoverable within 30 days of cancellation. After 30 days, customer information is periodically deleted for housekeeping purposes.

As mentioned, Auvik usually keeps some anonymized metadata from your account for the purpose of analyzing and optimizing our system performance.

If you prefer that network data from your account not be included in our aggregated metadata set, let our support team know when you make your cancellation request. In that case, we'll manually delete all information about your account from our system. The deletion will be permanent and the information will not be restorable.

METADATA

Metadata are records derived from or generated by network information. They include items such as network size, the connection speed between two devices, and Auvik's performance within a particular environment.

MORE QUESTIONS?

Have a question about Auvik or our system security that's not answered here? Give us a call. Or send an email. We're happy to talk to you.

1-866-59-AUVIK (28845) | North America

+44 (0)203 884 1655 | UK & Europe

+61 2 9159 8088 | Australia & New Zealand

security@auvik.com

ABOUT AUVIK

Auvik's cloud-based network management software keeps IT networks around the world running optimally. By automating and simplifying network management, Auvik helps rocket an IT team's efficiency and capacity, while protecting the business from network risk.