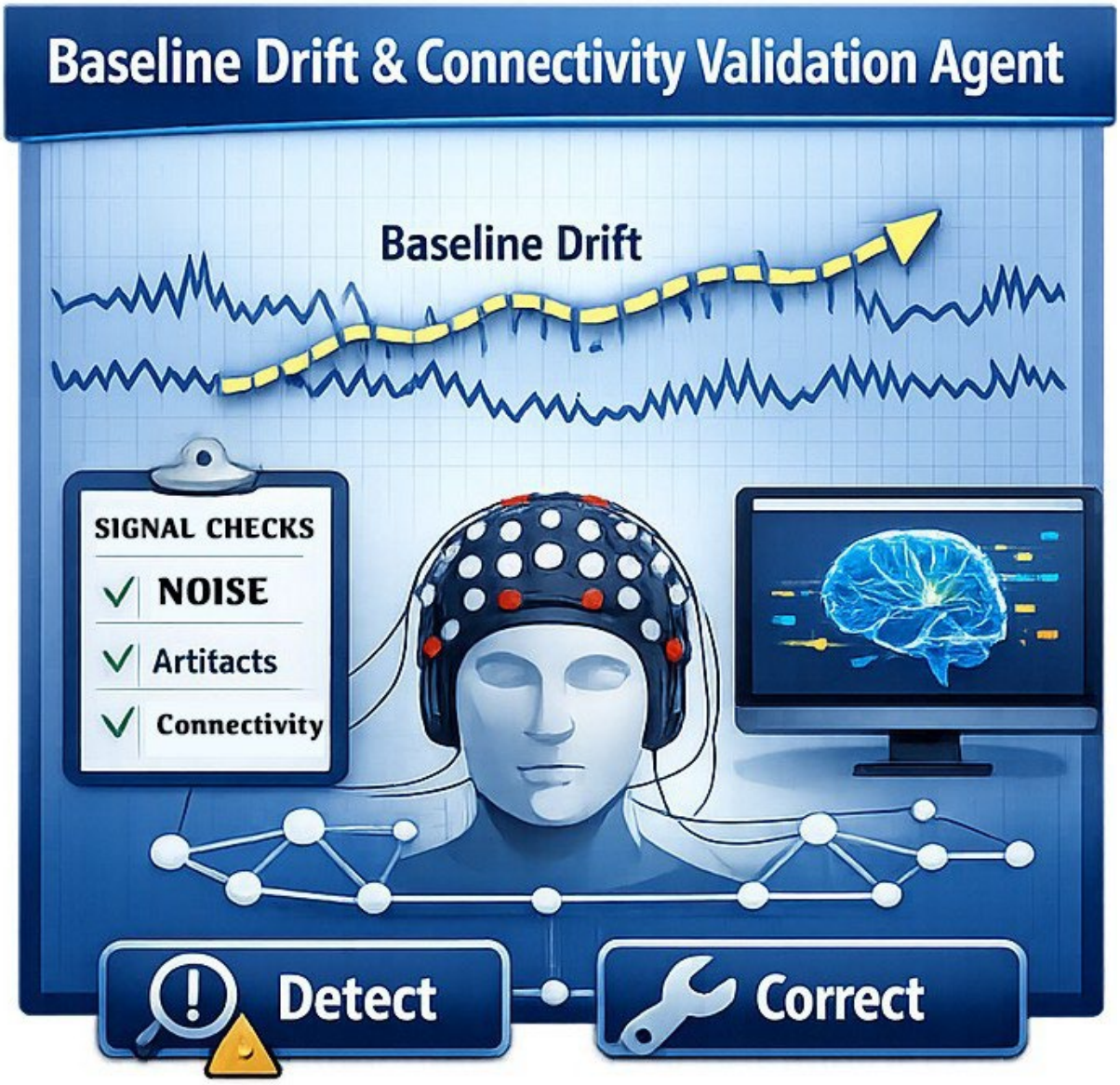
BaselineIQ v1.3 RC6.1 Customer Installation Guide



6/14/2026

Contents

Overview

Think about all the technology you use every day—websites, online games, streaming services, school systems, and mobile apps. Behind the scenes, all these things depend on computers and networks being able to communicate with each other.

BaselineIQ is a tool that helps IT teams make sure those connections keep working correctly. It regularly checks important computers, servers, websites, and network devices to see if anything has changed or stopped working.

You can think of BaselineIQ as a security guard that never sleeps. It continuously watches important systems and alerts IT staff when something looks different or broken.

BaselineIQ can detect:

- Connectivity failures – A computer or website can no longer be reached.
- DNS changes – A website or server name points to a different address than before.
- Route changes – Network traffic is taking a different path through the network.
- Traceroute changes – The devices that data passes through have changed.
- Latency increases – Connections are becoming slower than normal.
- Environmental drift – Something in the environment has changed from the expected configuration.

A Simple Example

Imagine your school has an online learning website. Yesterday everything worked perfectly, but today students cannot log in.

BaselineIQ might discover that:

- The website's server is offline.
- The server's address changed unexpectedly.
- Network traffic is taking a broken route.
- The connection has become much slower than normal.

Instead of waiting for users to complain, BaselineIQ helps IT teams find and fix problems faster by constantly checking for changes and warning them when something is wrong.

Glossary of Terms

This glossary explains common BaselineIQ terms using simple language.

Agent

The Agent is a helper program that performs checks on targets and sends the results to the database.

Think of it as: A helper that does the work for you.

Alert

An alert is a message sent when BaselineIQ finds a problem or important change.

Think of it as: A warning that tells someone to take a look.

Baseline

A baseline is a saved picture of how a target normally looks and behaves. Future checks are compared against the baseline to detect changes.

Think of it as: A picture of your clean room that helps you notice when something has moved.

Connectivity Check

A connectivity check verifies whether a target can be reached and is responding.

Think of it as: Knocking on a door and waiting to see if someone answers.

Dashboard

The Dashboard is the main page that shows the overall health of your monitored targets.

Think of it as: A report card that shows how everything is doing.

DNS

DNS (Domain Name System) translates names such as websites and servers into IP addresses that computers can use.

Think of it as: A phone book for computers.

Drift

Drift occurs when something changes from the saved baseline.

Think of it as: Noticing that a toy has been moved since you last cleaned your room.

Incident

An incident is a problem detected by BaselineIQ that may require attention.

Think of it as: Something that needs to be fixed.

Latency

Latency is the amount of time it takes for information to travel to a target and back.

Think of it as: How long it takes to ask a question and hear the answer.

Path

A path is the route that information takes to reach a target.

Think of it as: The roads and turns you take to get somewhere.

Route

A route is network information that helps determine how data reaches a target.

Think of it as: Directions on a map.

Snapshot

A snapshot is a record of the information collected during a check.

Think of it as: A picture of what was found at a specific moment.

Target

A target is a computer, server, website, network device, or other resource that BaselineIQ monitors.

Think of it as: Something we want to keep an eye on.

Traceroute

A traceroute shows each stop that information makes while traveling to a target.

Think of it as: Following a road trip and writing down every city you pass through.

Target Health

Target Health indicates whether a target is operating normally or experiencing issues.

Think of it as: A quick checkup to see if everything is okay.

Validation

Validation is the process of confirming that a target is reachable and behaving as expected.

Think of it as: Making sure everything is working the way it should.

Website Drift

Website drift occurs when a website's DNS information, connectivity, route, or path changes from its baseline.

Think of it as: Noticing that the way to your friend's house suddenly changed.

Windows Service

The Alert Service is a Windows Service that sends notifications when incidents occur.

Think of it as: A helper that works quietly in the background.

Included Components

BaselineIQ v1.3 RC4 RC6.1 includes:

- BaselineIQ.Console
- BaselineIQ.Agent
- BaselineIQ.AlertService
- SQL Server Database Objects
- Online Licensing Platform
- Customer License Activation and Deactivation

System Requirements Operating System Supported:

- Windows Server 2019
- Windows Server 2022
- Windows 10/11 (evaluation and lab use)

SQL Server
Supported:

- SQL Server Express 2019+
- SQL Server 2019+
- SQL Server 2022+

IIS
Required:

- Web Server (IIS)
- ASP.NET Core Hosting Bundle (.NET 8)

Installation

Run BaselineIQ_Setup.exe as Administrator.

The installer supports the following components:

- BaselineIQ Console
- BaselineIQ Database
- BaselineIQ Agent
- BaselineIQ Alert Service Recommended:

☑ Console
☑ Database
☑ Agent
☑ Alert Service

Installing Components on Different Machines

If you are installing BaselineIQ components on separate machines, keep the following in mind:

- The BaselineIQ Console installation requires access to the SQL Server instance so it can create the IIS Application Pool account and grant the necessary database permissions.
- The BaselineIQ Agent installation requires access to the SQL Server instance so it can create the Agent service account and grant the necessary database permissions.
- The SQL Server account used during installation must have sufficient privileges to create logins, users, and database role memberships.

This ensures that all BaselineIQ components can securely access the Console database and function correctly after installation.

Installation Locations

Program Files:
C:\Program Files\NETBASELINEIQ\BaselineIQ.Console
C:\Program Files\NETBASELINEIQ\BaselineIQ.Agent
C:\Program Files\NETBASELINEIQ\BaselineIQ.Agent.Updater
C:\Program Files\NETBASELINEIQ\BaselineIQ.AlertService

ProgramData:
C:\ProgramData\NETBASELINEIQ
C:\ProgramData\NETBASELINEIQ\Updates

First Login

Browse to:

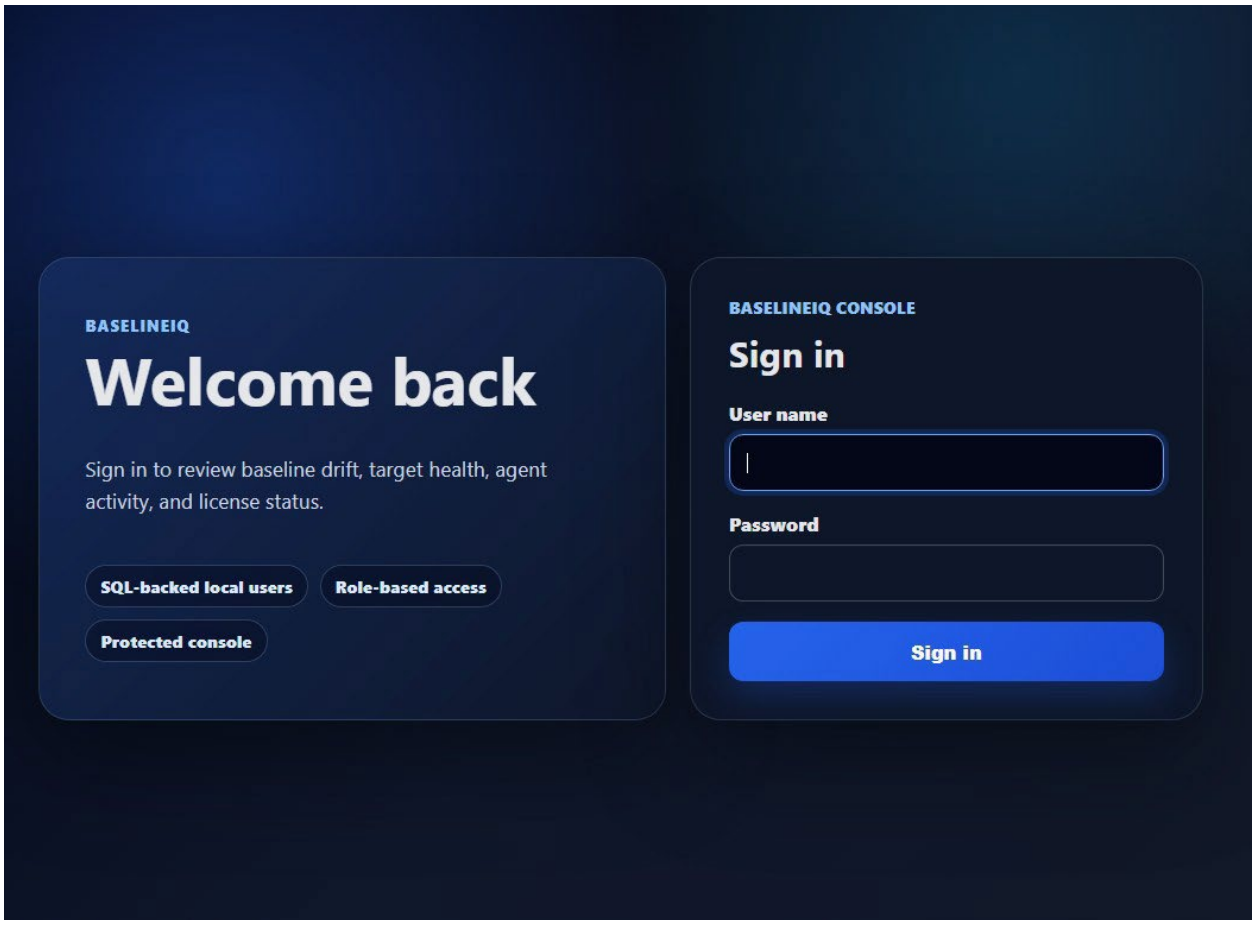
http://localhost:8085

During installation, BaselineIQ creates an initial administrator account.

The user name and generated password is displayed at the end of installation and saved to:

C:\ProgramData\NETBASELINEIQ\BaselineIQ_AdminCredentials.txt

Change the default password immediately after first login.



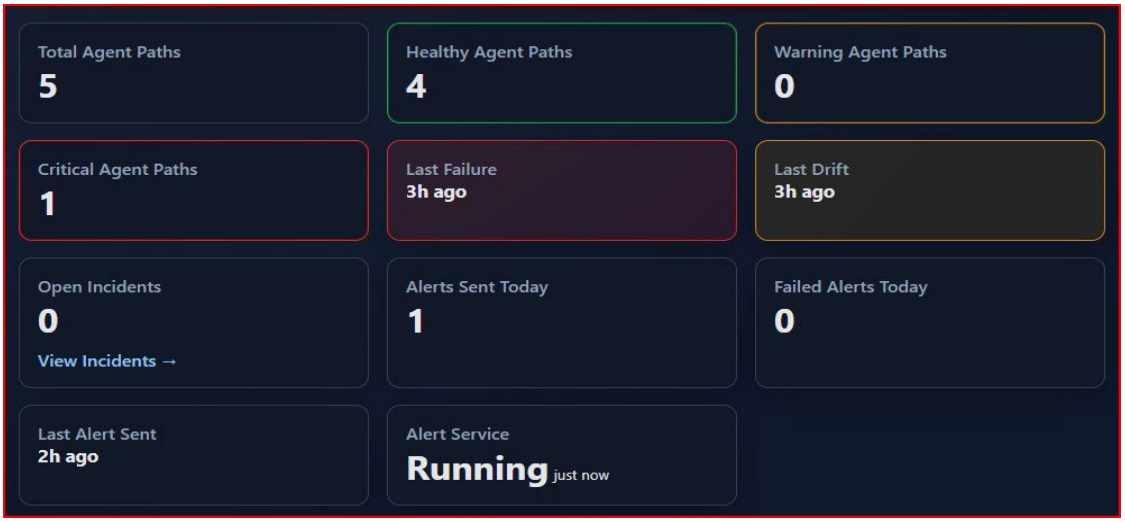
Dashboard

The Dashboard provides a quick overview of the health of your monitored environment. It is the first page displayed after logging in and is designed to help administrators quickly identify outages, drift events, and monitoring issues.

The Dashboard summarizes information collected by the BaselineIQ Agent and processed by the BaselineIQ Alert Service.

Dashboard Cards

Recent incidents can be reviewed directly from the Dashboard and prioritized using severity, operational impact, and incident assessment information.



Dashboard Item	Description
Healthy Paths	Number of targets currently operating normally.
Warning Paths	Targets that have detected drift or non-critical issues.
Critical Paths	Targets experiencing connectivity failures or critical conditions.
Open Incidents	Incidents that have not yet been resolved.
Alerts Sent Today	Number of alert notifications successfully sent during the current day.
Failed Alerts Today	Number of alert delivery attempts that failed.
Last Alert Sent	Date and time the most recent alert notification was delivered.
Alert Service Status	Current status of the BaselineIQ Alert Service.

What to Look For

A healthy environment will typically show:

- Most targets in the Healthy category
- Few or no Open Incidents
- Alert Service Status reporting Healthy
- Successful target checks being recorded regularly

Administrators should investigate:

- Increasing Critical Path counts
- Large numbers of Open Incidents
- Failed alert deliveries
- Alert Service Status showing Unknown or Offline

Typical Daily Workflow

- Open the Dashboard.
- Review Healthy, Warning, and Critical counts.
- Review any Open Incidents.
- Verify the Alert Service Status is Healthy.
- Investigate any newly detected drift or connectivity failures.

Recommended Practice

The Dashboard should be reviewed daily to verify that monitoring is functioning correctly and that important application paths remain healthy. A quick review of the Dashboard can often identify issues before they are reported by users.

Path Summary

The Path Summary section provides a quick view of the overall health of all monitored targets.

A path represents the complete network journey between the BaselineIQ Agent and a monitored target. This includes DNS resolution, network routing, connectivity validation, latency measurements, and traceroute information.
Each target is evaluated and assigned a health status based on the most recent monitoring results.

Path Statuses

Status	Description
Healthy	The target is reachable and no significant drift or connectivity issues have been detected.
Warning	The target is reachable, but BaselineIQ has detected drift or a non-critical condition that should be reviewed.
Critical	The target is unreachable or a significant problem has been detected that may impact service availability.

Why Path Summary Matters

The Path Summary allows administrators to quickly determine:

- How many monitored targets are operating normally
- Whether connectivity failures exist
- Whether environmental drift has been detected
- Which targets require immediate attention

Rather than reviewing every target individually, the Path Summary provides a high-level view of the overall health of the environment.

Example

If BaselineIQ is monitoring 20 targets:

- 18 Healthy
- 1 Warning
- 1 Critical

This indicates that most monitored paths are operating normally, one path has detected drift or a minor issue, and one path requires immediate investigation.

Recommended Practice

Review the Path Summary first when opening the Dashboard. If any Warning or Critical paths are present, investigate the affected targets and associated incidents to determine the cause and appropriate corrective action.

Current Target Status

The Current Target Status section displays the most recent monitoring results collected for a specific target.

This information helps administrators quickly determine whether a target is operating normally or experiencing connectivity issues, drift, or performance degradation.

The Current Target Status is updated each time the BaselineIQ Agent performs a monitoring check.

Current Target Status

Status	Target	Agent	Host	Port	Role	Last Check UTC	TCP	Latency	Drift	Last Failure	Error
Critical	DEV	M9_PROD	JKPAIDEV	445	DEV PC	36m ago (2026-06-14 18:06:17)	OK	1 ms	Yes (33)	3h ago (2026-06-14 15:06:24)	-
OK	ARRIS	M9_PROD	192.168.0.1	80	GATEWAY	36m ago (2026-06-14 18:06:17)	OK	1 ms	No	n/a	-
OK	COX	M9_PROD	cox.com	80	ISP	36m ago (2026-06-14 18:06:17)	OK	17 ms	No	n/a	-
OK	HP8020	M9_PROD	10.0.0.8	80	PRINTER	36m ago (2026-06-14 18:06:17)	OK	1 ms	No	n/a	-
OK	RAX41	M9_PROD	routerlogin.net	80	ROUTER	36m ago (2026-06-14 18:06:17)	OK	1 ms	No	n/a	-

Information Displayed

Depending on the target type and collected data, the Current Target Status section may display:

- Overall Health Status
- DNS Resolution Results
- TCP Connectivity Status
- Network Latency
- Route Information
- Traceroute Information
- Last Check Time
- Recent Drift Events

Health Status Indicators

Current Target Status

Status	Target	Agent	Host	Port	Role	Last Check UTC	TCP	Latency	Drift	Last Failure	Error
Critical	DEV	M9_PROD	JKPAIDEV	445	DEV PC	28m ago (2026-06-14 18:06:17)	OK	1 ms	Yes (33)	3h ago (2026-06-14 15:06:24)	-
OK	ARRIS	M9_PROD	192.168.0.1	80	GATEWAY	28m ago (2026-06-14 18:06:17)	OK	1 ms	No	n/a	-
OK	COX	M9_PROD	cox.com	80	ISP	28m ago (2026-06-14 18:06:17)	OK	17 ms	No	n/a	-
OK	HP8020	M9_PROD	10.0.0.8	80	PRINTER	28m ago (2026-06-14 18:06:17)	OK	1 ms	No	n/a	-
OK	RAX41	M9_PROD	routerlogin.net	80	ROUTER	28m ago (2026-06-14	OK	1 ms	No	n/a	-

Status	Description
Healthy	The target is reachable and operating within expected parameters.
Warning	Drift or a non-critical issue has been detected.
Critical	The target is unreachable or experiencing a significant issue.

What to Review

When investigating a target, review:

- Whether DNS is resolving correctly
- Whether the configured port is responding
- Whether latency has increased significantly
- Whether network routes have changed
- Whether traceroute results differ from the baseline
- Whether active incidents are associated with the target

Example

A website target may show:

- DNS Resolution: Successful
- TCP Connectivity: Successful
- Latency: 22 ms
- Route Status: Normal
- Traceroute Status: Normal
- Overall Status: Healthy

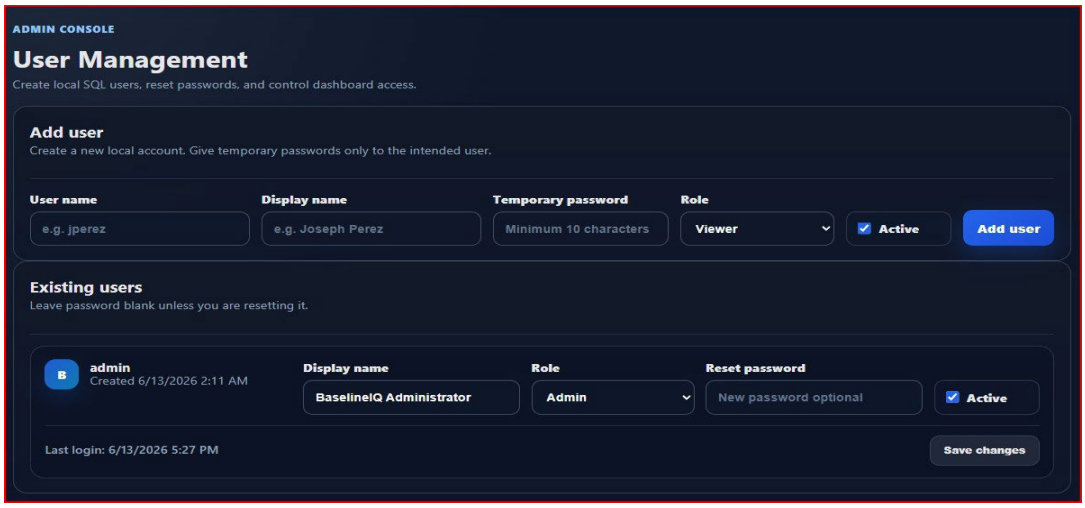
If the website later becomes unreachable, the Current Target Status may change to Critical and an incident may be created automatically.

Recommended Practice

When reviewing incidents or alert notifications, use the Current Target Status section as the starting point for troubleshooting. It provides the most recent information collected by the BaselineIQ Agent and often identifies the source of the problem quickly.

Managing Users

BaselineIQ includes built-in user management that allows administrators to control access to the Console.



Navigate to: Users From this page you can:

- Create new users
- Modify existing users
- Enable or disable accounts
- Assign roles
- Reset passwords
- View user activity information

Creating a User

To create a new user:

1. Navigate to User Management.
2. Click Add User.
3. Enter:
4. Username
5. Display Name
6. Password
7. Role
8. Click Save.

The user can immediately sign in using the credentials provided.

User Roles

BaselineIQ supports role-based access control.

Role	Description
Administrator	Full access to all BaselineIQ features, configuration, licensing, users, targets, incidents, and alerting.
Operator	Can view dashboards, incidents, target information, and monitoring results.
Viewer	Read-only access to monitoring information and dashboards.

Disabling a User

Accounts can be disabled without deleting them.

Disabled users:

- Cannot log in
- Retain historical audit information
- Can be re-enabled later

Password Management

Administrators can reset passwords for existing users from the User Management page.
For security reasons:

- Use strong passwords
- Change default passwords after installation
- Disable accounts that are no longer required

Recommended Practice

Create individual accounts for each administrator rather than sharing a common account.

This provides:

- Better accountability
- Easier auditing
- Improved security

Initial Administrator Account

The installer creates the initial administrator account and generated password during installation and is displayed in a notepad window when setup completes. You can find the credentials in C:\ProgramData\NETBASELINEIQ\BaselineIQ_AdminCredentials.txt

Change the password immediately after first login.

Licensing

Every installation begins in Trial mode.

Trial

- 5 Active Targets
- 30 Day Trial

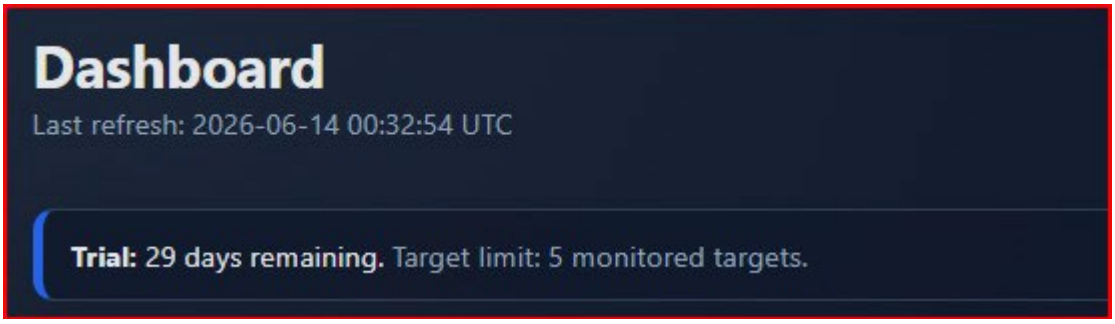
Professional

- 25 Active Targets
- Online Activation
- One Year of Updates

To purchase a professional license, visit https://www.netbaselineiq.com/Buy

Enterprise

- Contact Sales



License Activation

Professional licenses may be activated on a machine using the License Management page.

If a license must be moved to another system:

1. Navigate to Administration → Licensing.
2. Click Deactivate License.
3. Confirm the deactivation.
4. The Console returns to Trial mode.
5. The license key may then be activated on another system.

License Deactivation

Professional licenses can be deactivated directly from the License Management page.

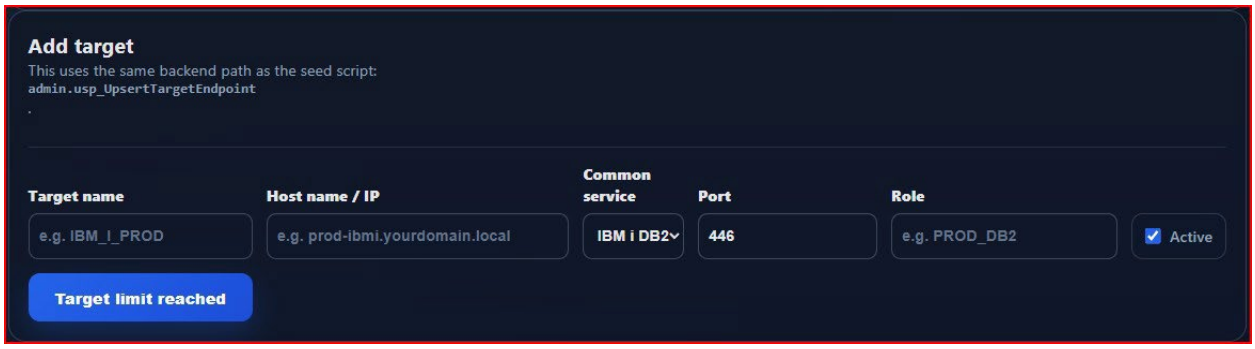
This allows a license to be transferred to another system without contacting support.

When a license is deactivated:

- Local activation data is removed
- The installation reverts to Trial mode
- The license key becomes available for activation elsewhere

Adding Targets

A target is a computer, server, website, or network device that you want BaselineIQ to monitor. The BaselineIQ Agent checks the target regularly and logs its status and any changes it detects to the database.



Navigate to: Manage Targets Examples:

- Websites
- Routers
- Printers
- Application Servers
- SQL Servers
- Storage Devices

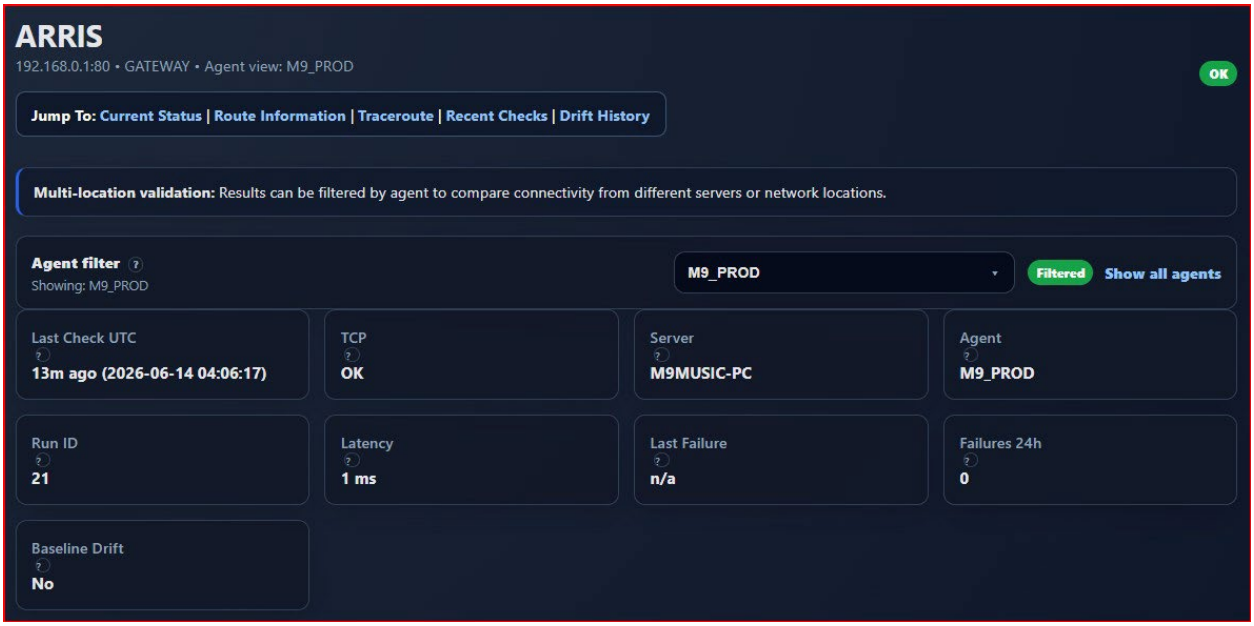
DNS Services Assign:
- Target Name
- Host Name / IP
- Port
- Role

Initial Baseline Collection

After adding targets:
1. Run the BaselineIQ Agent.
2. Allow the Agent to collect initial target information.
3. Review Target Details.
4. Verify baseline information has been collected.

BaselineIQ requires an initial baseline before drift detection can occur.

Example Target Results



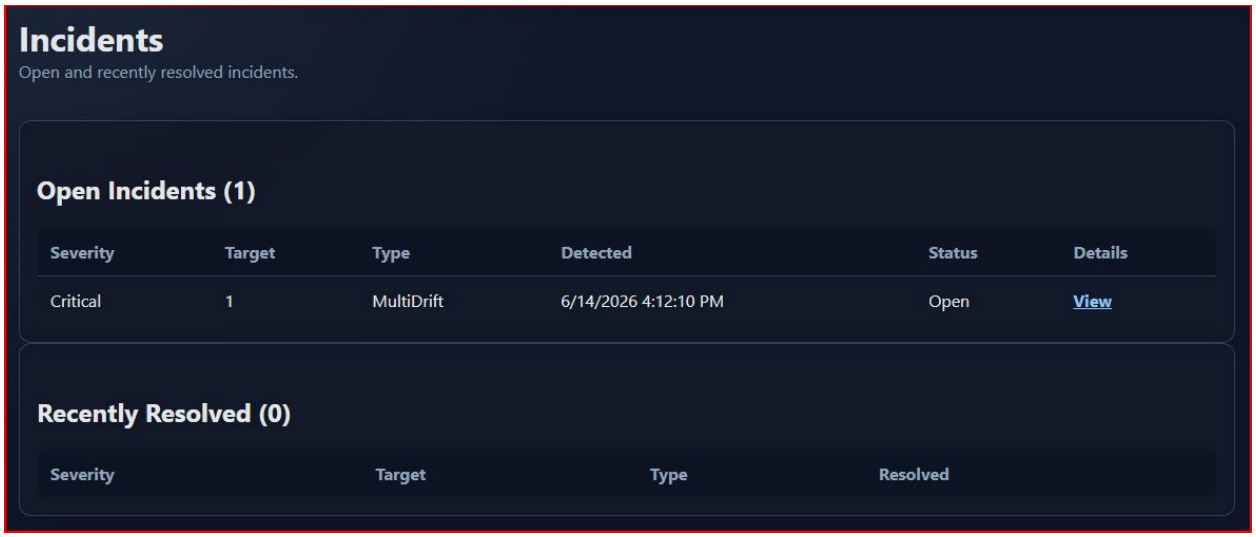
The Target Details page should display:

- DNS Results
- TCP Results
- Latency Information
- Route Information
- Traceroute Information
- Recent Checks

Incidents

An Incident is a problem detected by BaselineIQ that may require attention from an administrator or support team.

When the BaselineIQ Agent discovers a connectivity failure or detects environmental drift, BaselineIQ automatically creates an incident record. Incidents help administrators track problems from the time they are detected until they are resolved.



Navigate to:

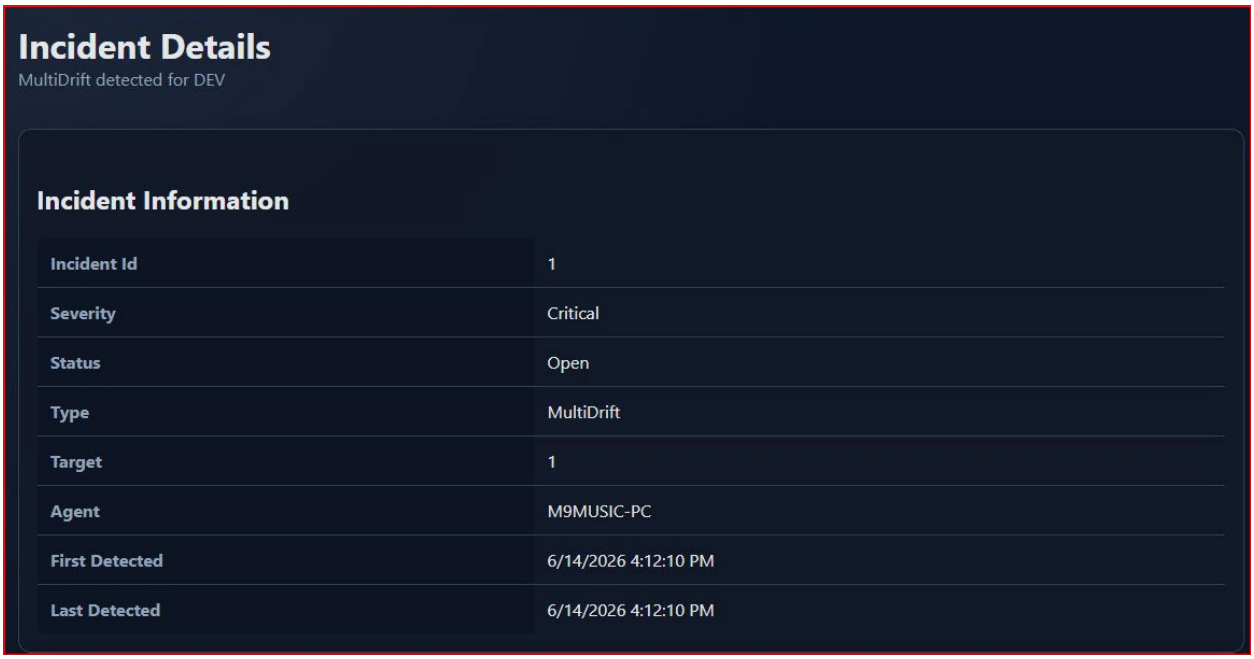
Incidents

The Incidents page displays all active and historical incidents detected by BaselineIQ.

An incident may be created when:

- A target becomes unreachable
- A monitored port stops responding
- DNS information changes
- Route information changes
- Traceroute information changes
- Latency exceeds expected values
- Environmental drift is detected

Incident States



State	Description
Open	A problem has been detected and still exists.
Resolved	The condition has returned to normal and the incident has been automatically resolved.

Incident Information

Each incident includes information such as:

- Incident Type
- Severity
- Target Name
- Detection Time
- Resolution Time
- Description of the detected change
- Alert Delivery Status

Incident Assessment

BaselineIQ automatically analyzes each incident and provides an Incident Assessment to help administrators quickly understand what happened.

The Incident Assessment may include:

- Likely Cause
- Operational Impact
- Recommended Action
- Confidence Score
- Related Activity
- Common Cause Analysis

Rather than requiring administrators to interpret raw monitoring data, BaselineIQ summarizes the most likely explanation for the detected change and recommends an appropriate response.

Common Cause Analysis

When multiple monitored targets experience similar changes within a short period of time, BaselineIQ can identify related activity and suggest a likely common cause.

Examples include:

· DNS provider updates
· Internet routing changes
· Cloud service infrastructure changes
· Network provider outages

This helps administrators determine whether several incidents are part of the same underlying event rather than unrelated problems.

Severity Levels

Severity	Description
Critical	Major outage or connectivity failure requiring immediate attention.
High	Significant drift or degradation that could affect service availability.
Medium	Important change that should be reviewed.
Information	Minor changes recorded for awareness and auditing purposes.

Incident Lifecycle

Target Check Performed
↓
Problem or Drift Detected
↓
Incident Created
↓
Alert Service Sends Notification
↓
Issue Corrected
↓
Incident Automatically Resolved

Recommended Practice

Review open incidents regularly and investigate recurring incidents that repeatedly open and resolve. Frequent incidents may indicate unstable network paths, intermittent connectivity problems, DNS changes, or infrastructure issues that require corrective action.

Contributing Events

Category	Field	Summary
DNS	ResolvedAddresses	ResolvedAddresses disappeared for DEV. Previous value: 10.0.0.19,fe80::14df:5856:7382:2a18%10
Connectivity	TcpSucceeded	TcpSucceeded changed for DEV. Baseline: True Current: False
Route	DestinationPrefix	DestinationPrefix disappeared for DEV. Previous value: 10.0.0.0/24
Route	NextHop	NextHop disappeared for DEV. Previous value: Direct / same subnet
Route	RouteMetric	RouteMetric disappeared for DEV. Previous value: 281
Route	InterfaceAlias	InterfaceAlias disappeared for DEV. Previous value: Ethernet
Route	InterfaceIndex	InterfaceIndex disappeared for DEV. Previous value: 10
Traceroute	HopSummary	HopSummary disappeared for DEV. Previous value: 10.0.0.19
Traceroute	HopCount	HopCount disappeared for DEV. Previous value: 1
Traceroute	ReachedTarget	ReachedTarget changed for DEV. Baseline: True Current: False

BaselineIQ Agent

The BaselineIQ Agent is responsible for performing all connectivity validation and data collection activities within BaselineIQ. It serves as the monitoring engine that gathers information about your environment and stores the results in the BaselineIQ database.

The Agent periodically checks each configured target and records:

- DNS resolution results
- TCP connectivity status
- Network latency
- Route information
- Traceroute information

The collected data is stored in the BaselineIQ database where it is displayed throughout the application, including:

- Dashboard
- Target Details
- Incidents
- Drift History
- Reports

A scheduled task created during installation automatically runs the Agent at the configured interval. The same execution cycle is used to periodically check for approved Agent updates published through the BaselineIQ Console.

Understanding Agent Location

The location of an Agent can significantly affect the monitoring results that are collected. Network paths often differ depending on where a connection originates. A target that is reachable from one location may be unreachable from another, or the route used to reach the target may vary between locations.
For this reason, BaselineIQ supports deploying multiple Agents throughout your environment.

Single-Agent Deployments

In a simple deployment, a single Agent may be installed on a server within the primary data center or server network.

Example:

BaselineIQ Agent
│
├── SQL Server
├── Web Server
├── Domain Controller
└── Internet Websites

This approach provides visibility from a single network location and is often sufficient for smaller environments.

Multi-Agent Deployments

Larger organizations may deploy Agents in multiple locations. Examples include:

- Different offices
- Different VLANs
- Different subnets
- Different data centers
- Cloud environments

Disaster Recovery sites Example:

Agent - Corporate Office Agent - Data Center Agent - Branch Office
Agent - Azure Environment

Each Agent performs connectivity validation from its own network perspective.

Why Multiple Agents Matter

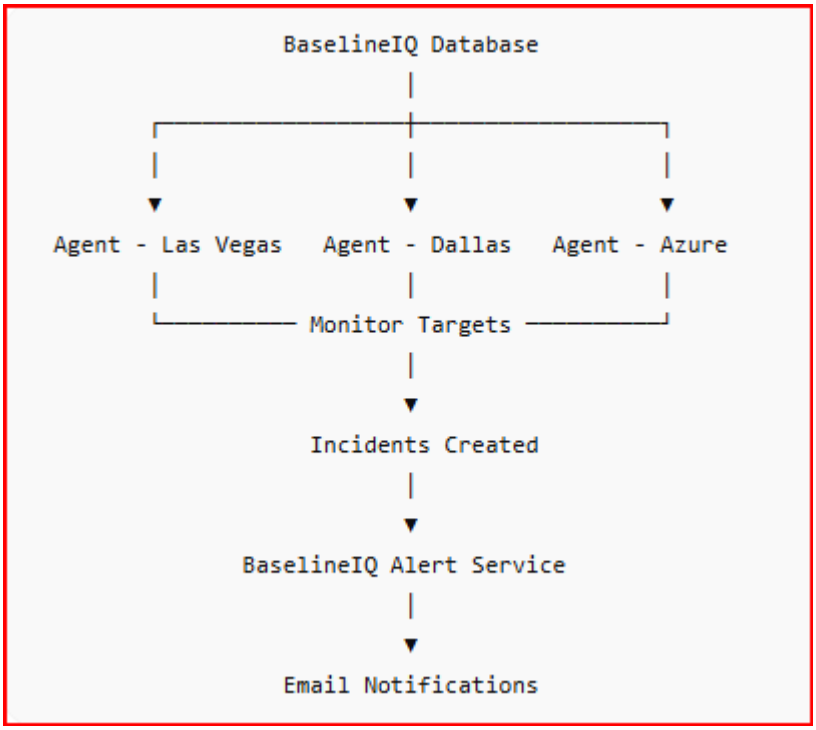
Consider a web server located in a DMZ.
An Agent located inside the corporate network may successfully reach the server, while an Agent located in a branch office may encounter a routing issue.

Similarly:

- DNS results may differ between locations.
- Routes may differ between locations.
- Latency may differ between locations.
- Internet providers may use different network paths.

By deploying multiple Agents, administrators gain visibility into how applications and services are performing from different parts of the environment.

Multi-Agent Diagram



Dashboard Visibility

When multiple Agents are deployed, BaselineIQ records which Agent collected each result. Dashboard information can be filtered by Agent, allowing administrators to view:

- Health status by Agent
- Open incidents by Agent
- Connectivity results by Agent
- Drift events by Agent

This makes it possible to determine whether a problem is affecting:

- One location
- Several locations
- The entire organization

Filter by Agent

When multiple BaselineIQ Agents are deployed, the Dashboard includes a Filter by Agent dropdown that allows administrators to view monitoring data from a specific Agent.
By default, the Dashboard displays results from all Agents.

Selecting an Agent filters Dashboard information to show only the results collected by that Agent, including:

- Path Summary
- Open Incidents
- Target Status
- Drift Events
- Monitoring Results

This allows administrators to isolate issues affecting a particular location, subnet, office, data center, or cloud environment.

Example

A company has Agents installed in:

- Las Vegas
- Sacramento
- Dallas

Users in Sacramento report application connectivity issues. An administrator can select:

Filter by Agent → Sacramento
The Dashboard will then display only the monitoring results collected by the Sacramento Agent, making it easier to determine whether the issue is isolated to that location or affecting multiple sites.

Recommended Practice

When investigating an incident, first determine whether the issue appears across all Agents or only a specific Agent location. Problems visible from only one Agent often indicate local network, routing, firewall, ISP, or DNS issues rather than a complete application outage.

Example Scenario

A company has three offices:

- Las Vegas
- Sacramento
- Dallas

An Agent is installed in each location.
A DNS change occurs for a critical application. Results may appear as:

Agent Location	Result
Las Vegas	New DNS address detected
Sacramento	New DNS address detected
Dallas	Original DNS address still resolving

This immediately indicates that the change may be related to DNS replication or geographic DNS services rather than an application outage.

Agent Identity

Each Agent reports its own identity information to the database, including:

- Agent Name
- Host Name
- Agent Location
- Collection Time

This information is displayed throughout the Dashboard, Target Details, Incidents, and Drift History pages so administrators can easily determine where monitoring results originated.

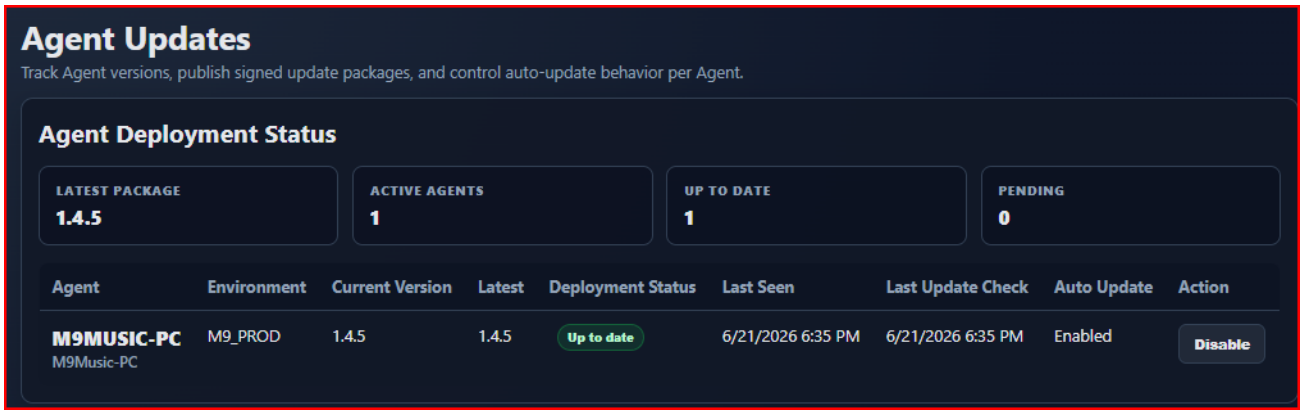
Recommended Practice

Deploy Agents as close as possible to the users, applications, or network segments you want to monitor.

For critical systems, consider installing Agents in multiple locations. Monitoring the same target from different network perspectives often provides earlier detection of routing issues, firewall changes, WAN outages, DNS inconsistencies, and other environmental drift that may not be visible from a single location.

Agent Auto-Updates

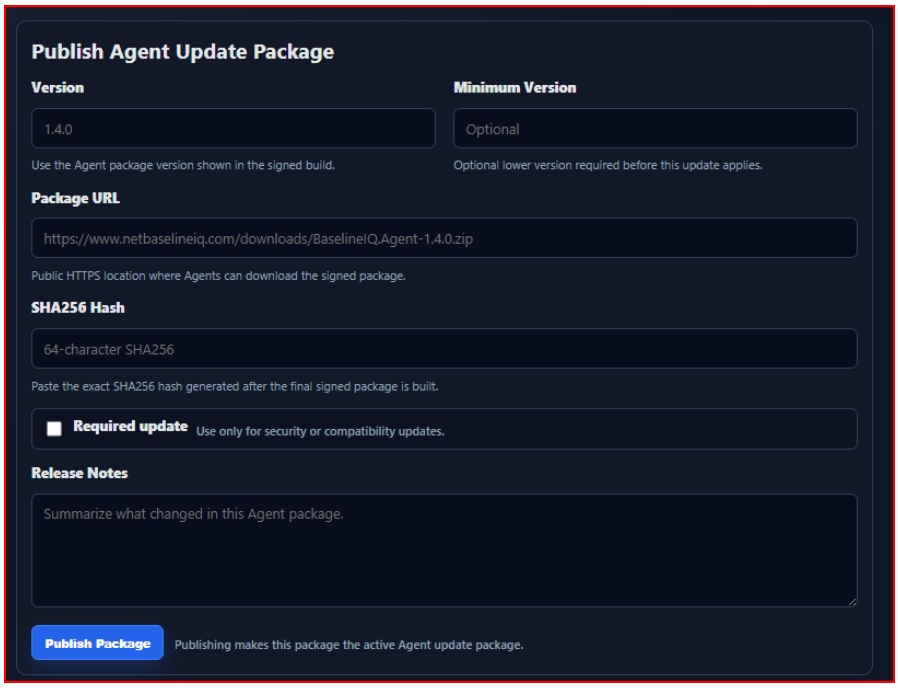
BaselineIQ supports centralized Agent updates.



When a newer Agent version is published by an administrator, Agents periodically check for available updates.

If an update is available:

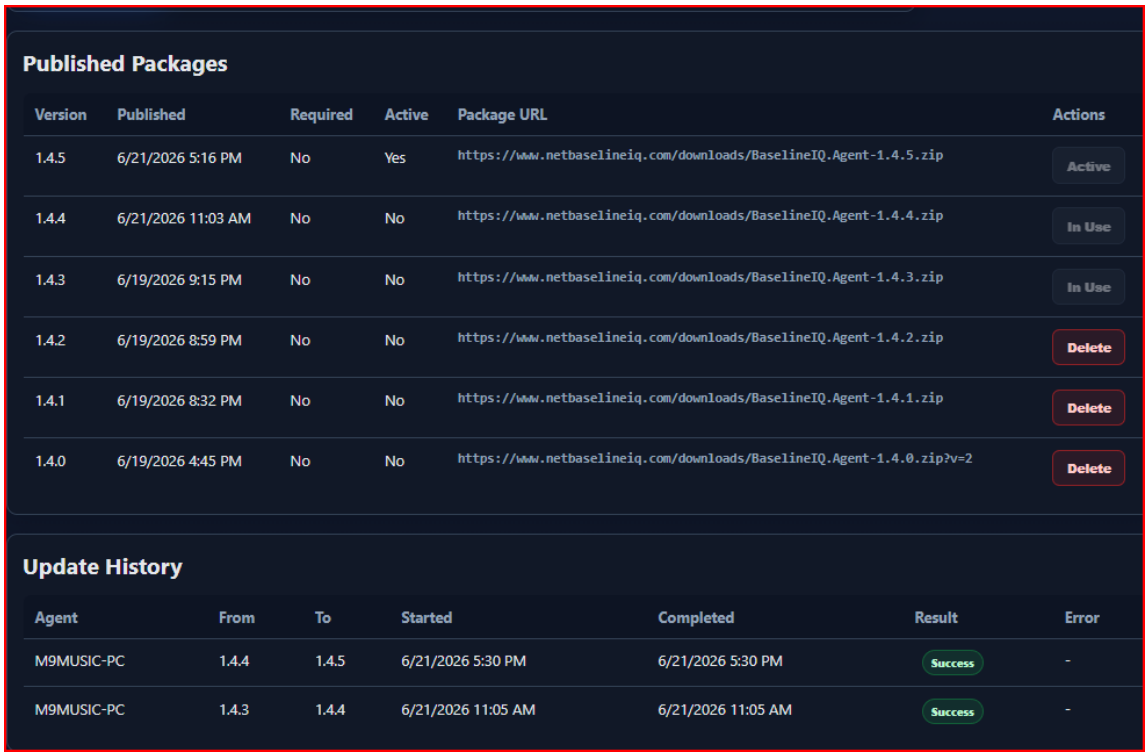
1. The Agent downloads the update package.
2. The package SHA256 hash is verified.
3. Files are staged locally.
4. BaselineIQ.Agent.Updater performs the upgrade.
5. The Agent resumes normal operation.



Benefits:

- Reduced maintenance effort
- Consistent Agent versions
- Simplified multi-agent deployments

- Improved deployment reliability
- Update package integrity validation using SHA-256 hashes
- Centralized update administration through the BaselineIQ Console



Published Packages

Version	Published	Required	Active	Package URL	Actions
1.4.5	6/21/2026 5:16 PM	No	Yes	https://www.netbaselineiq.com/downloads/BaselineIQ.Agent-1.4.5.zip	Active
1.4.4	6/21/2026 11:03 AM	No	No	https://www.netbaselineiq.com/downloads/BaselineIQ.Agent-1.4.4.zip	In Use
1.4.3	6/19/2026 9:15 PM	No	No	https://www.netbaselineiq.com/downloads/BaselineIQ.Agent-1.4.3.zip	In Use
1.4.2	6/19/2026 8:59 PM	No	No	https://www.netbaselineiq.com/downloads/BaselineIQ.Agent-1.4.2.zip	Delete
1.4.1	6/19/2026 8:32 PM	No	No	https://www.netbaselineiq.com/downloads/BaselineIQ.Agent-1.4.1.zip	Delete
1.4.0	6/19/2026 4:45 PM	No	No	https://www.netbaselineiq.com/downloads/BaselineIQ.Agent-1.4.0.zip?v=2	Delete

Update History

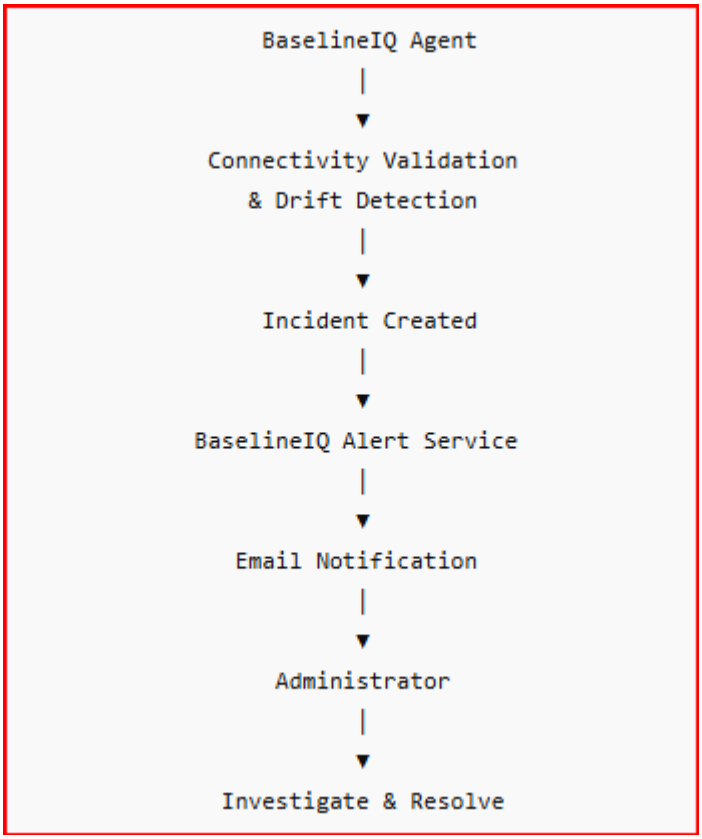
Agent	From	To	Started	Completed	Result	Error
M9MUSIC-PC	1.4.4	1.4.5	6/21/2026 5:30 PM	6/21/2026 5:30 PM	Success	-
M9MUSIC-PC	1.4.3	1.4.4	6/21/2026 11:05 AM	6/21/2026 11:05 AM	Success	-

BaselineIQ Alert Service

The BaselineIQ Alert Service is responsible for processing incidents and delivering email notifications to administrators and support personnel.

While the BaselineIQ Agent performs monitoring and data collection, the Alert Service is responsible for notifying people when problems occur.

Diagram



The Alert Service runs independently of the Dashboard.

Incident creation, scoring, and email processing continue even when no users are logged into the Console.

The relationship between the components is: BaselineIQ Agent
↓
Connectivity Failure or Drift Detected
↓
Incident Created

↓
Alert Service Detects Incident
↓
Email Notification Sent
↓
Administrator Investigates Issue

The Alert Service continuously monitors the BaselineIQ database for newly created incidents and automatically sends notifications to configured Alert Recipients.

The Alert Service:

- Monitors open incidents
- Sends incident notifications
- Sends incident resolution notifications
- Prevents duplicate notifications
- Tracks delivery status
- Records service heartbeat information
- Generates alert processing statistics displayed on the Dashboard

Relationship to the Dashboard

Several Dashboard components rely directly on the Alert Service. The Dashboard displays:

- Alert Service Status
- Alerts Sent Today
- Failed Alerts Today
- Last Alert Sent

These values help administrators verify that alert processing is functioning correctly.

For example:

- If an incident exists but Alerts Sent Today remains at zero, the Alert Service may not be running.
- If Failed Alerts Today increases, SMTP configuration or email delivery should be investigated.
- If Alert Service Status displays Unknown or Offline, administrators should verify that the Alert Service is running and able to communicate with the database.

Service Heartbeat Monitoring

The Alert Service periodically records a heartbeat in the database.
The Dashboard uses this heartbeat information to determine whether the service is healthy and actively processing incidents.

A healthy heartbeat indicates:

- The service is running
- Database connectivity is working
- Incident processing is operational

Why the Alert Service Is Important

Without the Alert Service, BaselineIQ will continue collecting monitoring data and creating incidents, but administrators will not receive email notifications.

In other words:

- The Agent discovers problems.
- Incidents record problems.
- The Alert Service informs people about problems.

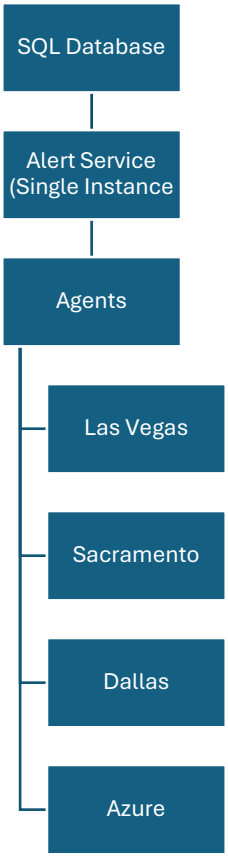
All three components work together to provide complete monitoring and alerting capabilities.

Alert Service Deployment Recommendations

Unlike the BaselineIQ Agent, which can be installed on multiple systems throughout the environment, the BaselineIQ Alert Service is typically installed as a single instance.

Recommended:

- One Alert Service per BaselineIQ environment
- Multiple Agents as needed Example:



Why Only One Alert Service?

The Alert Service processes incidents and sends notifications on behalf of the entire BaselineIQ environment.

Running multiple Alert Service instances against the same database can result in:

- Duplicate alert emails
- Duplicate resolution notifications
- Increased database activity
- Unpredictable alert processing behavior

Because all incidents are stored centrally in the BaselineIQ database, only a single Alert Service is required to process notifications for all monitored targets and all Agents.

How It Differs from the Agent

The Agent collects monitoring data from a specific network location. Additional Agents provide

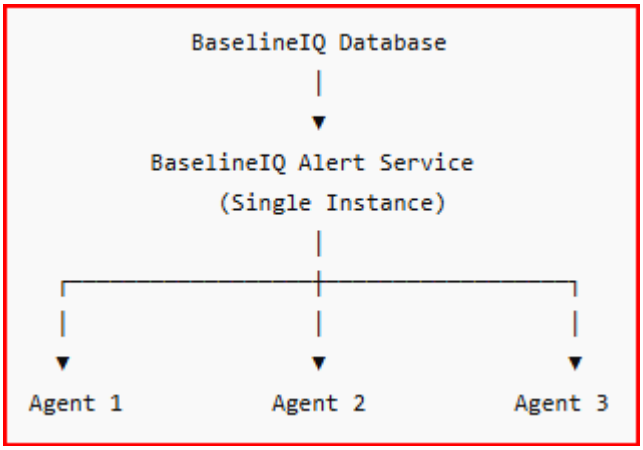
additional visibility.

The Alert Service does not collect monitoring data and does not provide additional monitoring coverage. Its purpose is to process incidents that already exist in the database and deliver notifications.

For this reason:

- Deploy multiple Agents when additional monitoring perspectives are needed.
- Deploy a single Alert Service to process notifications.

Alert Service Deployment Diagram



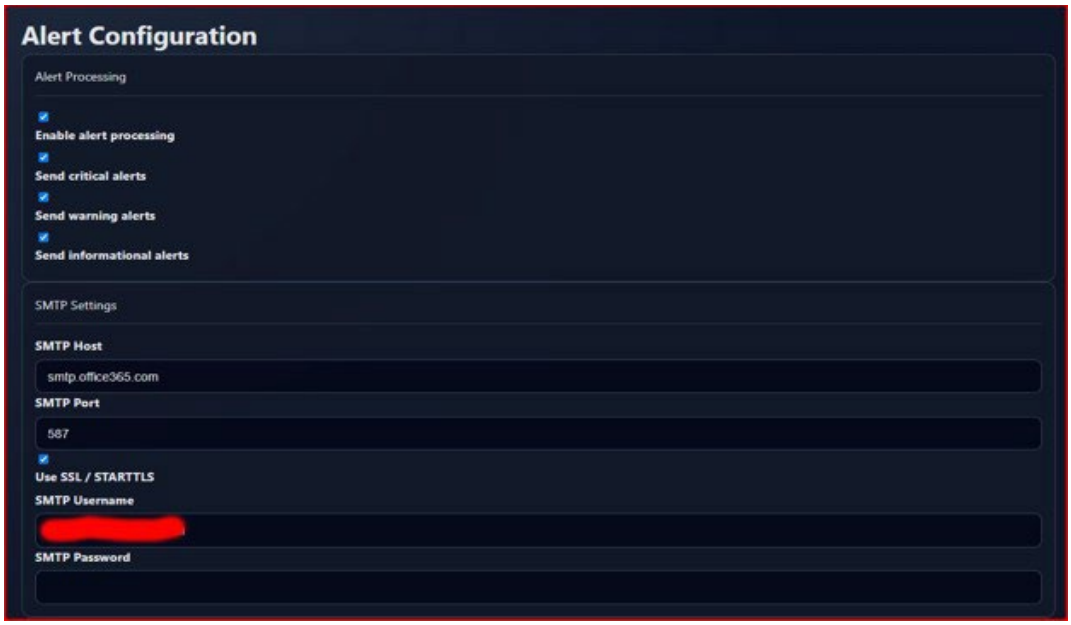
Alerting Overview

BaselineIQ creates incidents when connectivity failures or drift events are detected.

The Alert Service monitors these incidents and sends email notifications to configured Alert Recipients using the SMTP settings configured on the Alert Configuration page.

Alert Configuration

The Alert Configuration page controls how BaselineIQ sends email notifications.

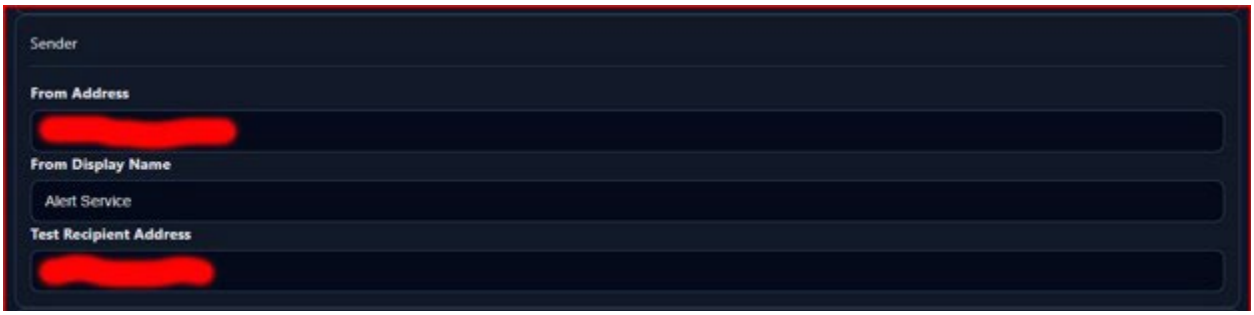


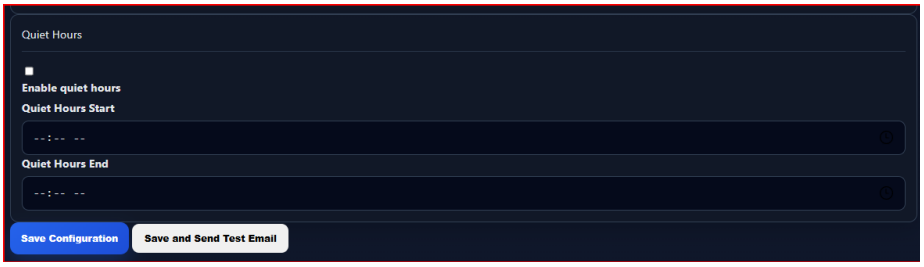
Navigate to: Administration → Alert Configuration Configure the following settings:

Setting	Description
SMTP Host	Mail server hostname used to send email notifications
SMTP Port	SMTP port number (typically 587 for Microsoft 365)
Use SSL	Enables encrypted SMTP communication
From Address	Email address displayed as the sender
From Display Name	Friendly name shown to email recipients

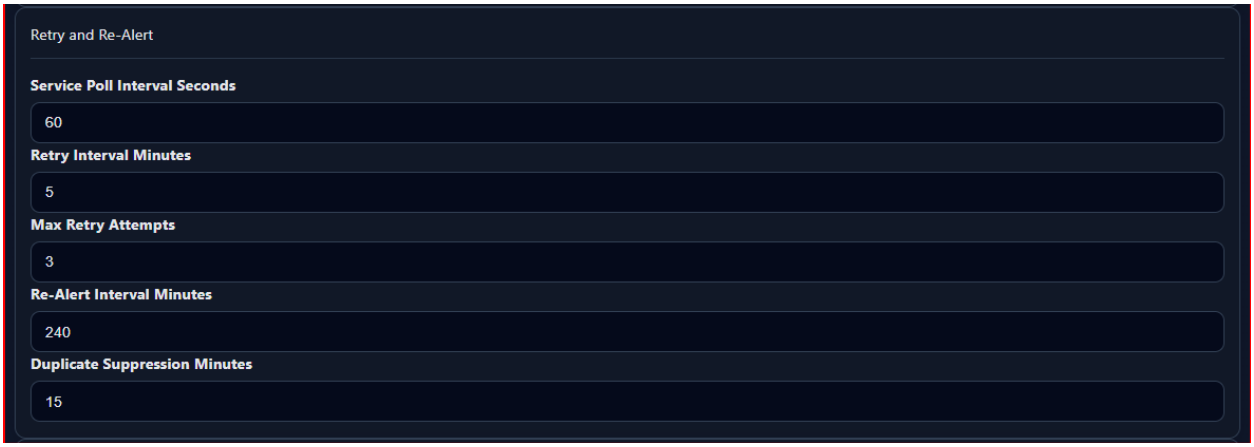
Setting	*Description*
SMTP Username	SMTP account used for authentication
SMTP Password	SMTP account password
Test Recipient Address	Recipient used when sending test emails

After saving the configuration, use Send Test Email to verify that email delivery is working correctly.





Alert Processing Settings



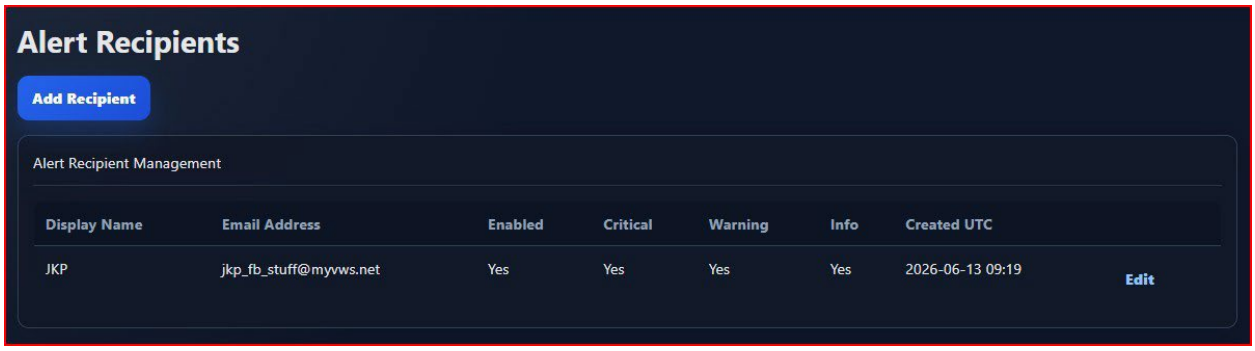
The Alert Service uses the following configuration values:

Setting	Recommended Value
Service Poll Interval Seconds	60
Retry Interval Minutes	5
Max Retry Attempts	3
Re-Alert Interval Minutes	240
Duplicate Suppression Minutes	15

These settings control how frequently the Alert Service processes incidents and sends notifications.

Alert Recipients

Alert Recipients determine who receives email notifications when BaselineIQ detects a connectivity failure, outage, or drift event.



Navigate to: Administration → Alert Recipients

Add one or more recipients. For each recipient specify:

Setting	Description
Display Name	Friendly recipient name
Email Address	Destination email address
Enabled	Determines whether the recipient receives alerts

Example Recipients

Network Operations Team noc@company.com

Infrastructure Team infrastructure@company.com

IT Manager itmanager@company.com

Testing Alert Delivery

After configuring recipients:

1. Configure SMTP settings on the Alert Configuration page.
2. Send a test email.
3. Verify the email is received successfully.
4. Confirm the recipient appears in the Alert Recipients list and is enabled.

Alert Workflow

Connectivity Failure or Drift
↓
Incident Created
↓
Alert Service Detects Incident
↓
Email Notification Sent
↓
Alert Recipients Receive Email

If no recipients are configured, BaselineIQ will continue monitoring and recording incidents, but no email notifications will be delivered.

Uninstalling BaselineIQ

BaselineIQ can be removed using Apps & Features or the Uninstall BaselineIQ shortcut.

By default, uninstalling BaselineIQ removes:

- BaselineIQ Console files
- BaselineIQ Agent files
- BaselineIQ Alert Service files
- Windows Services installed by BaselineIQ
- Scheduled Tasks installed by BaselineIQ
- IIS Sites and Application Pools created by BaselineIQ

To prevent accidental data loss, the following items are preserved:

- NetBaseline database
- ProgramData configuration and log files
- SQL logins and permissions created during installation

If complete removal is required, administrators may run the Cleanup-BaselineIQ-Leftovers.ps1 utility after uninstalling the product.

Warning:

Removing the NetBaseline database permanently deletes:

- Monitoring history
- Baselines
- Incidents
- Alert history
- Configuration data

This action cannot be undone.

Troubleshooting

Dashboard Shows No Results Verify:

- Agent installed
- Scheduled task exists
- SQL connectivity
- Active targets configured

Alert Service Shows Unknown

Verify:

- Alert Service running
- ServiceHeartbeat table populated
- SQL permissions configured

License Activation Issues

Verify:

- Internet connectivity
- Access to licensing.netbaselineiq.com
- Valid license key

Agent Update Issues

Verify:

- Console Base URL is configured correctly
- Agent can reach the BaselineIQ Console
- Update package SHA256 hash is valid
- Update package URL is accessible
- Update staging folder exists
- BaselineIQ.Agent.Updater is installed

Support

Website: https://netbaselineiq.com

Email: support@netbaselineiq.com

Product Updates

Updated installers, release notes, and product documentation are available from:
https://www.netbaselineiq.com/download
Customers should periodically review release notes for bug fixes, enhancements, and security updates.

Document Version: BaselineIQ v1.3 RC4 RC6.1