

NEWBRIDGE IAM

Identity & Access Management – RADIUS and Captive Portal, Cloud or On-Premise



IDENTITY

GUEST ACCESS

GATEWAY

Carrier-grade AAA and guest onboarding from one console – authenticate employees, issue vouchers to visitors, onboard BYOD devices, and run branded captive portals across every site, with an optional on-premise Gateway when internet access management belongs inside the building.

5

IDENTITY CLASSES

16

REPORT TEMPLATES

Cloud

OR ON-PREMISE

IDENTITY & AUTHENTICATION

- Permanent users, vouchers, BYOD devices and social logins in one directory
- Policy profiles binding bandwidth, quota and session limits per identity class
- Realms, NAS devices and called-station rules for multi-site AAA

GUEST ACCESS

- Branded captive portals with a terms-and-conditions editor
- Portal surveys capturing structured visitor data
- Advertisement campaigns with per-campaign performance reporting

ARCHITECTURE & SCALE

- Cloud subscription or on-premise appliance, same console
- Optional on-premise Gateway for internet access management
- Split-plane design: user traffic never leaves the site

EVIDENCE & CONTROL

- 16 report templates across RADIUS and captive portal
- Session detail records, usage by user, and voucher lifecycle
- Role-based access control, applied per cloud or per site

INTRODUCTION

Newbridge IAM delivers the RADIUS and Captive Portal modules of the Newbridge platform. It answers two questions every network has to answer: who is this user, and what are they allowed to do.

RADIUS handles authentication, authorization and accounting for permanent users, vouchers, BYOD devices and social logins, with policy profiles that bind each identity class to a bandwidth, quota and session policy. Captive Portal handles the guest experience: branded splash pages, surveys, advertisement campaigns and a terms-and-conditions editor.

Run IAM as a cloud subscription, or on-premise on a Newbridge appliance where identity data must stay inside the building. The console and the feature set are the same in both. Add the optional Gateway appliance on-premise when the deployment also needs internet access management at the edge.

Newbridge IAM enables the **RADIUS** and **Captive Portal** modules. Wi-Fi management is delivered by **Newbridge Controller**; the complete module set is **Newbridge CMC**.

ADVANTAGES

Identity and guest access are usually two systems that disagree with each other. Newbridge IAM makes them one, under a single policy engine and a single audit trail.

One identity directory

Permanent users, vouchers, BYOD devices and social logins live in one place, under one policy engine. No second system to reconcile.

Guests onboard themselves

Voucher batches, one-time passes and self-service portals remove the front-desk bottleneck. Print a batch, hand it out, walk away.

Policy, not per-user fiddling

Profiles bind bandwidth, quota and session limits to a class of identity. Change the profile, every user in it moves.

Deploy it your way

The same console and feature set as a cloud subscription or an on-premise appliance. A deployment choice, not a feature trade.

Identity data can stay home

On-premise deployments keep the user directory, session records and portal data inside the building.

Internet access management, optionally

Add the Gateway appliance on-premise for firewall, DHCP, DNS forwarding, hotspot and web services at the edge.

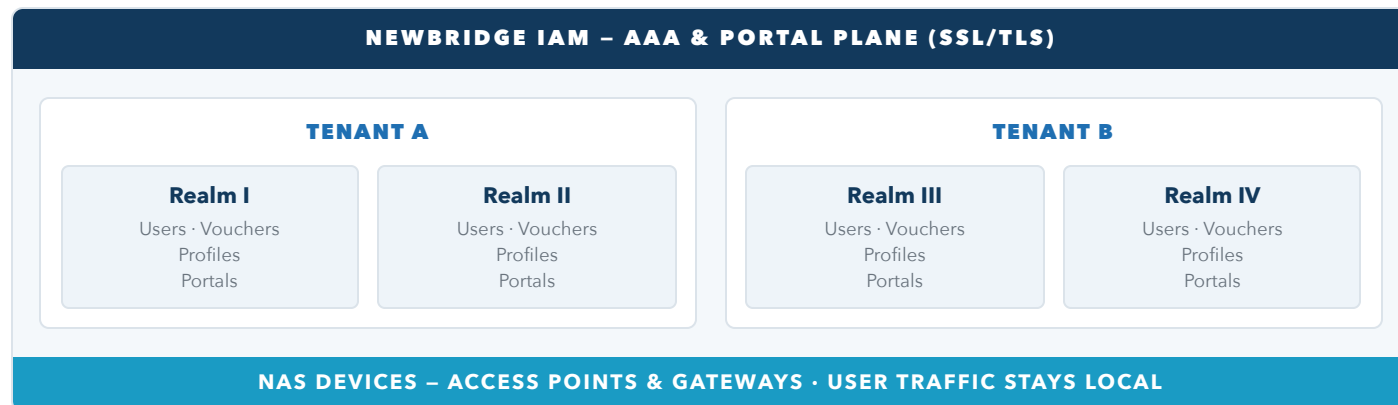
Evidence for the audit

Authentication audits, session detail records (CDR), data-cap breaches and idle-session reports, on demand or scheduled.

Know what the campaign did

Advertisement performance, survey responses, and new-versus-returning visitor breakdowns per portal.

ARCHITECTURE



Each tenant is isolated. Authentication requests are routed by realm and matched by called station. Only management and accounting data reaches the control plane.

CLOUD OR ON-PREMISE

The RADIUS and Captive Portal modules are identical in both deployments. What differs is where the control plane runs, and whether internet access management sits at the edge.

	CLOUD	ON-PREMISE
Control plane	Newbridge-hosted, serverless	Newbridge appliance
Console	Identical web interface	Identical web interface
Identity data	Held in the cloud tenant	Held inside the building
Capacity	Max Online Users, Max Portals	Licence-controlled, bounded by the appliance
Optional Gateway	–	NB-IAMG appliance
User traffic	Stays local	Stays local

ON-PREMISE APPLIANCES

IAM runs on the same appliance family as Newbridge Controller, ordered with the IAM licence. Capacity is licence-controlled by Max Online Users and Max Portals, not by managed access points.

ORDER NO.	APPLIANCE
NB-9180-IAM-UK	Newbridge 9180-class appliance, IAM licence
NB-9480-IAM-UK	Newbridge 9480-class appliance, IAM licence
NB-9980-IAM-UK	Newbridge 9980-class appliance, IAM licence

OPTIONAL GATEWAY

The Gateway is an on-premise appliance that adds the On-Premise module: network interfaces and routes, firewall, DNS forwarder, DHCP server, hotspot and web server. It also provides captive portal, internet load balancing and NAT firewalling at the edge.

ORDER NO.	CONCURRENT DEVICES
NB-IAMG-980	Up to 980
NB-IAMG-2980	Up to 2,980
NB-IAMG-4980	Up to 4,980

THE NEWBRIDGE MANAGEMENT FAMILY

NEWBRIDGE CONTROLLER	NEWBRIDGE IAM	NEWBRIDGE CMC
Wi-Fi management: the Network Controller module, cloud or on-premise. SEPARATE PRODUCT	Identity and guest access: the RADIUS and Captive Portal modules. THIS DATASHEET	The complete module set: Network Controller, RADIUS, Captive Portal and On-Premise services. OPTIONAL GATEWAY ON-PREMISE

IDENTITY CLASSES

- **Permanent Users** – named accounts for staff and long-lived identities, each bound to a policy profile.
- **Voucher Batches** – generate vouchers in bulk for events, conferences and retail, with a shared expiry and policy.
- **Single Vouchers (One-Time Pass)** – individually issued credentials for a single visit.
- **Devices (BYOD)** – MAC-based authentication for devices that cannot present credentials.
- **Social Users** – identities established through a social login on the captive portal.

POLICY PROFILES

- **Profile Listing** – every policy in the tenant, with the identity classes bound to it.
- **New Profile Wizard** – guided creation of a policy from bandwidth, quota and session components.
- **Components** – reusable policy fragments composed into profiles.
- Change the profile, and every identity bound to it moves with it.

NETWORK

OBJECT	PURPOSE
NAS Devices	The access points, controllers and gateways permitted to send RADIUS requests
Realms	Route authentication requests by realm, for multi-tenant and roaming deployments
Called Stations	Match requests by called-station identifier, binding policy to an SSID or a site

RADIUS DASHBOARD

A live authentication and accounting overview: active sessions, authentication outcomes, and the identity classes in use across the tenant. Accounting records feed the session-detail and usage reports without a separate collector.

PORTAL MANAGEMENT

- **Portal Dashboard** – sessions, logins and onboarding outcomes across every portal in the tenant.
- **Portals** – branded splash pages, one per site or per SSID, with configurable login methods.
- **Portal Surveys** – structured questions presented during onboarding, with responses exported to report.
- **Portal Advertisements** – campaigns presented on the splash page, measured by impression and click-through.
- **Terms & Conditions** – a versioned editor; acceptance is recorded against the session.

ONBOARDING FLOW

1

Associate

The guest joins the SSID and is redirected to the branded portal.

2

Identify

Voucher, social login, BYOD device or permanent account; terms accepted and recorded.

3

Authorize

RADIUS applies the policy profile: bandwidth, quota and session limits.

ALERTS, LOGS & AUTOMATION

- **Email alerts** – raised on events that need attention
- **Notifications** – event alerting with configurable recipients
- **Audit trail** – operation, configuration, client and connection logs
- **Scheduler jobs** – background task monitoring for recurring work
- **Report schedules** – recurring generation with archived downloads
- **Role-based access control** – permissions applied per cloud or per site

FEATURE MAP – RADIUS & CAPTIVE PORTAL MODULES

IDENTITIES

Permanent users Voucher batches
Single vouchers Devices (BYOD)
Social users

POLICY

Profile listing Add profile
New profile wizard Components

RADIUS NETWORK

NAS devices Realms Called stations
RADIUS dashboard

CAPTIVE PORTAL

Portal dashboard Portals
Portal surveys Advertisements
Terms & conditions

REPORTS

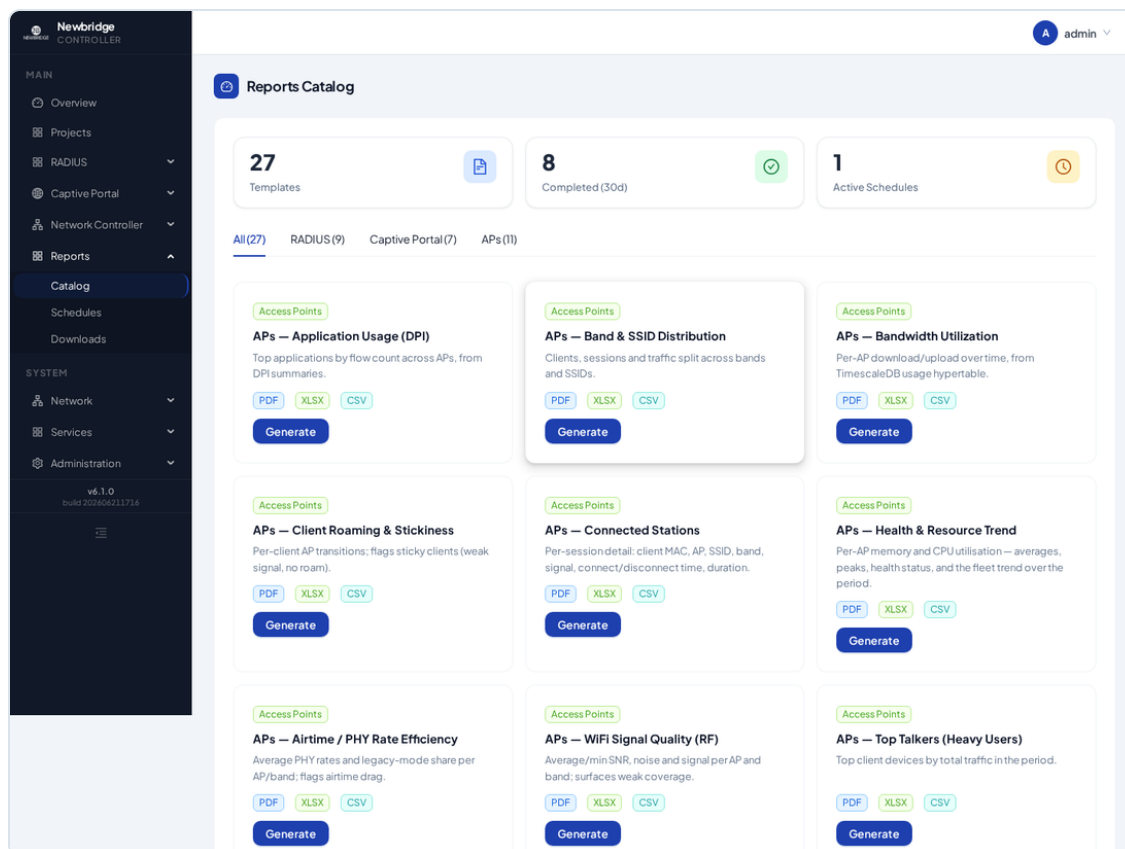
Reports catalog 16 templates
Recurring schedules PDF · XLSX · CSV

ADMINISTRATION

General settings Notifications
User accounts Roles & permissions
Scheduler jobs Licence management

REPORTS CATALOG

Sixteen report templates ship with the RADIUS and Captive Portal modules. Generate any of them on demand, or put them on a recurring schedule and collect the output from the downloads archive. Every template exports to PDF, XLSX or CSV.



Reports catalog – templates by category, each generating to PDF, XLSX or CSV.

RADIUS REPORTS

- **Authentication Audit** – accept and reject outcomes over time, by user, NAS and realm
- **Concurrent Sessions / Peak** – concurrency over time, with the peak and when it occurred
- **Data-Cap / Quota Breach** – identities that crossed their profile's data allowance
- **Idle / Stale Session Audit** – sessions held open without traffic; flags accounting gaps
- **NAS / Site Utilization** – authentication load and session count per NAS device and site
- **Realm / Roaming Summary** – requests routed by realm; roaming volume between sites
- **Session Detail (CDR)** – per-session call detail records: identity, NAS, duration, octets
- **Usage by User** – total upload, download and session time per identity
- **Voucher Batch Report** – issued, redeemed, expired and unused vouchers per batch

CAPTIVE PORTAL REPORTS

- **Portal Activity** – sessions, logins and unique visitors per portal
- **Advertisement Performance** – impressions and click-through per campaign
- **Login-Method Breakdown** – split across voucher, social, BYOD and permanent-user logins
- **New vs Returning Visitors** – first-time against repeat visitors over the period
- **Guest Onboarding Funnel** – drop-off from splash view to authenticated session
- **Survey Responses** – structured answers collected during onboarding
- **Voucher Lifecycle** – issue, first use, last use and expiry per voucher

A further eleven access-point templates are delivered with Newbridge Controller.

SESSION RECORDS & RETENTION

- Per-session accounting: identity, NAS device, realm and called station
- Session duration, input and output octets
- Authentication outcomes, accept and reject, with reason
- Voucher state transitions: issued, redeemed, expired
- Portal acceptance records against the terms version in force
- Retention depends on licence type – two months or more

GRANULAR ACCESS CONTROL

ROLE	SCOPE
Administrator / Owner	Total authority over the environment and all associated sites
Site Manager	Full read/write privileges restricted to specific locations or departments
Guest / Viewer	Read-only access for monitoring and reporting, with no configuration rights

Roles and permissions are defined under Administration → User Management, and applied per cloud or per site.

SECURE & RESILIENT ARCHITECTURE

- **End-to-End Encryption** – all communication between on-premises devices and the control plane is protected with industry-standard SSL/TLS.
- **Separation of Planes** – only management and accounting data travels to the cloud; user traffic stays local.
- **Hardened Privacy** – rigorous access controls and data masking keep sensitive identity information private.
- **Tenant Isolation** – realms, portals and identity directories are scoped to their tenant.

LICENSING

The platform is licensed by module. Newbridge IAM enables the RADIUS and Captive Portal modules. Each licence carries its own validity period and capacity limits, is imported into the console as a file or as encrypted licence text, and more than one licence may be active at a time.

FIELD	DESCRIPTION
Enabled Modules	Which modules the licence activates
Valid Until	Expiry date of the licence; status is shown as Active or Expired
Max Online Users	Licence-controlled limit on concurrent authenticated users
Max Portals	Licence-controlled limit on captive-portal instances
Client Name	Organization the licence is issued to, shown per licence

Capacity limits are set per licence and enforced by the controller. The console reports application version, hardware serial, licence serial and overall status under Administration → Licence Management.

ENTITLEMENT AND THE GATEWAY

The Gateway is what enables the On-Premise module. An IAM appliance ordered without one runs RADIUS and Captive Portal; ordered with one, it additionally runs the On-Premise module's edge services. The two entitlements carry different appliance part numbers.

APPLIANCE ORDER CODE	MODULES ENABLED
NB-9x80-IAM-UK	RADIUS, Captive Portal
NB-9x80-IAMGW-UK	RADIUS, Captive Portal, On-Premise – Gateway required

Cloud deployments have no Gateway, so the On-Premise module is not available in the cloud.

CLOUD

ORDER NO.	DESCRIPTION
NB-CLD-IAM-1Y	Newbridge IAM cloud subscription, 1 year
NB-CLD-IAM-2Y	Newbridge IAM cloud subscription, 2 years
NB-CLD-IAM-3Y	Newbridge IAM cloud subscription, 3 years
NB-CLD-IAM-4Y	Newbridge IAM cloud subscription, 4 years
NB-CLD-IAM-5Y	Newbridge IAM cloud subscription, 5 years

ON-PREMISE APPLIANCE

ORDER NO.	DESCRIPTION
NB-9180-IAM-UK	Newbridge 9180-class appliance, IAM licence
NB-9480-IAM-UK	Newbridge 9480-class appliance, IAM licence
NB-9980-IAM-UK	Newbridge 9980-class appliance, IAM licence
NB-9180-IAMGW-UK	Newbridge 9180-class appliance, IAM licence with On-Premise module
NB-9480-IAMGW-UK	Newbridge 9480-class appliance, IAM licence with On-Premise module
NB-9980-IAMGW-UK	Newbridge 9980-class appliance, IAM licence with On-Premise module

GATEWAY

ORDER NO.	DESCRIPTION
NB-IAMG-980	Internet Access Management Gateway, up to 980 concurrent devices
NB-IAMG-2980	Internet Access Management Gateway, up to 2,980 concurrent devices
NB-IAMG-4980	Internet Access Management Gateway, up to 4,980 concurrent devices

An **IAMGW** appliance must be ordered with a Gateway. Cloud subscriptions are sized by concurrent authenticated users and captive-portal instances, and include Newbridge software and hardware support for the term. Appliances and gateways take a separate support contract, available in one- to five-year terms.

Newbridge and the Newbridge logo are trademarks of their respective owners. SDX LAB SDN BHD is the authorized principal of Newbridge products in Malaysia. All other company and product names may be trademarks of their respective companies. All specifications are subject to change without notice. Feature availability depends on the licence modules enabled and the controller software release deployed. Contact us at <https://www.newbridge-tech.com/>