COMMSCOPE®
RUCKUS ®

RUCKUS® Cloudpath® Enrollment System

Secure network access for BYOD, guest users and
IT-owned devices

COMPOSED OF:

- All-inclusive user-based license or subscription

DEPLOYMENT OPTIONS:

- Cloud-based
- Virtualized on-premises (VMware®, Hyper-V®)

BENEFITS

- Increases security for the network, devices, users and data
- Streamlines network onboarding for BYOD users, guests and IT-owned devices
- Gives you the power to define and manage policies for role-based access
- Delivers visibility and control over what devices are on the network
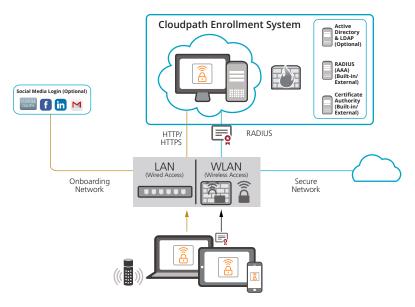- Dramatically reduces helpdesk tickets related to network access

FEATURES

- Secure network access
- Certificate management
- Self-service onboarding and device enablement
- Policy management
- Third-party product integration via APIs

RUCKUS® Cloudpath® Enrollment System is software/SaaS that delivers secure network access for any user, and any device, on any network.

Cloudpath secures every connection with WPA2/WPA3-Enterprise, protecting data in transit between the device and the access point with powerful encryption. You gain visibility and control over which devices are on the network, and can define and manage policies so every user sees only the network resources they should see. Cloudpath software checks the security posture of devices during onboarding to ensure they comply with your organization's security policies. The system redirects users with noncompliant devices to remediate them before granting access. It associates every device with a user, and you can easily revoke access at any time—for example, when a BYOD user leaves the organization.

Intuitive self-service workflows streamline network onboarding—users gain network access simply and securely without IT intervention. The software lets you deliver a great onboarding experience while dramatically reducing helpdesk tickets related to network access. Internal users can easily self-provision any device for network access using their existing login credentials. Cloudpath installs a digital certificate for network authentication so that, after the initial connection, users don't need to re-enter credentials when they connect again. Guest users access a self-service login portal and receive credentials for internet access via email or SMS.
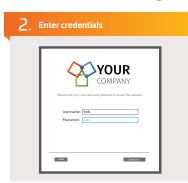
The Cloudpath service interoperates via its APIs with third-party products to further enhance security and improve user experience. It works flawlessly with any vendor's wired and wireless infrastructure. Unlike leading competitors, Cloudpath software offers a unique

Cloudpath Enrollment System delivers secure network access for any device and any user on any network.

Secure network onboarding workflow

1. Who are you? Internal user or guest?

2. Enter credentials

3. Download certificate

BYOD and guest users can easily onboard their devices for secure network access with intuitive self-service workflows—without IT intervention.

combination of cloud-based or virtualized on-premises deployment, built-in multi-tenancy, cost-effective per-user licensing, and superior ease of use.

Secure multi-vendor network access

Cloudpath software delivers secure network access for every user, and every device, on any vendor's network.

- Secure connections with WPA2/WPA3-Enterprise via 802.1X authentication
- Powerful encryption for data in transit over the air
- Support for BYOD, guest and IT-owned devices—including IoT devices
- Up-front-posture check with remediation
- Visibility and control over devices on the network—with the power to revoke access

Certificate management

Cloudpath software includes a built-in, comprehensive Certificate Authority (CA) that lets you create and manage your own Public Key Infrastructure (PKI).

- Built-in RADIUS server and user database
- Integration with external certificate authorities and user database infrastructures
- Certificate-based authentication, authorization and accounting (AAA)

Self-service onboarding and device enablement

Easy self-service onboarding ensures that users gain network access quickly and securely—without helpdesk involvement.

- Customizable workflows—entirely self-service or with internal sponsors—to tailor the user experience
- Optional pre-boarding lets users set up their devices for secure access before arriving at a given location

- Device provisioning capability can prompt users to install specific software during onboarding
- Customizable onboarding portal for guest access—including optional social login with Google, Facebook, LinkedIn and other popular identity providers
- Guest credentials via email, SMS or printed voucher

Policy management

Cloudpath software lets you define and manage policies that govern network access for all users. The software works with your network infrastructure to enforce policies for role-based access.

- Granular per-user, per-device policies, including bandwidth management and application-based access
- Role-based access—users get only the appropriate level of access
- Private per-user networks via VLANs or access policies—users see only their devices and traffic

Third-party product integration via API

Cloudpath software integrates via its APIs with third-party products to enhance security and user experience. It works with any product that can consume its APIs.

- Web content filters—lets these products filter encrypted content and apply role-based filtering rules (technology partnerships: iBoss® and Lightspeed Systems®)
- Next-generation firewalls—enables per-user and per-device policies (technology partnership: Palo Alto Networks®)
- Mobile device management—works with MDM products to support both managed and unmanaged devices with appropriate policies (technology partnership: AirWatch®)
- eduroam®—facilitates inter-campus roaming
- Google Chromebooks™—enables single-tap network onboarding

Specifications

Deployment options	• Cloud-based deployment • On-premises virtualized deployment (VMware or Hyper-V)
Redundancy and multi-tenancy	• VM-based Cloudpath Enrollment System can be deployed as a standalone server or as a cluster in both active-active mode or as a star-hub for data replication and redundancy • Multi-tenant mode enables MSPs to host multiple tenants within a single instance
Certificate infrastructure (PKI)	• Built-in certificate management system • Unique CA for every tenant within the multi-tenant mode • Ability to connect to external PKI • Standalone or subordinate to integrate with existing PKI • Certificate templates that integrate with policy • Supports OCSP with automatic revocation
RADIUS	• Support for dynamic VLANs, ACLs and more • Streamlined support for EAP-TLS and MAC Filtering • Client-based support for PEAP • Built-in RADIUS server • Ability to connect to an external RADIUS infrastructure • RADIUS accounting
Onboarding	• Self-service onboarding with customizable workflows • Support for wired/wireless infrastructure from any standards-based vendor • Unified wired or wireless access • Support for BYOD, guest, IT-owned assets—including IoT devices
Visibility and reporting	• Per-device and per-user visibility and control • Association between user, device, certificate and policy • RADIUS accounting
Authentication protocols	• 802.1X (EAP methods: EAP-TLS, PEAP [client only], DPSK™) • Web authentication • Non-802.1X (MAC authentication) • EAP-SIM configuration for iOS • Support for HS2.0 R1 and HS2.0 R2 via OSU (Online Signup Server) • Radius CoA • OAuth 2.0 and SAML 2.0 • DPSK configuration for RUCKUS WLAN
User identity support	• Microsoft® Active Directory® • RADIUS via PAP • Any LDAP-compliant directory • Novell® • Internal user database
Device support	• Android™ 4.3 and higher • iOS® 6.0 and higher • Chrome™ OS • Windows® XP and higher • Mac OS X 10.7 and higher • Ubuntu® 12.04 and higher • Fedora® 18 and higher • Windows Phone® 8.1 • BlackBerry®
SMS and email	• Native integration with Twilio® and CDYNE® • Ability to configure any custom SMS gateway • Built-in SMTP server or configure SMTP server
Third-party integrations via API	• Next-generation firewalls • Web content filters • Mobile device management • eduroam • Google Chromebooks • Any platform that can consume APIs

Licensing overview

Subscription

(Support included)

Cloud			
Step 1	Choose number of users		
<1K	1K–5K	5K–10K	10K+

Step 2	Choose subscription duration		
<1K	1 year	3 years	5 years

On-premises			
Step 1	Choose number of users		
<1K	1K–5K	5K–10K	10K+

Step 2	Choose subscription duration		
<1K	1 year	3 years	5 years

Step 3	Choose server license quantity
1 License per 20K users	

- Licensed by user, not device
- User count determines volume discount
- Separate list price for education customers

Perpetual license

Step 1	Choose number of users		
<1K	1K–5K	5K–10K	10K+

Step 2	Choose server license quantity
1 License per 20K users	

Step 3	Choose support duration		
<1K	1 year	3 years	5 years

- Licensed by user, not device
- User count determines volume discount
- Separate list price for education customers

Ordering guidance

1. Select from cloud or on-premises deployment model.

2. If you select on-premises, choose from subscription or perpetual licensing model.

3. Cloud deployment requires subscription model.

4. Determine the number of users in your environment, including guests.

5. Choose the appropriate SKU based upon subscription duration and user count.

6. Add optional white glove service for remotely assisted deployment.

Connection
we solve IT™

Contact an Account Manager to discuss how we can help increase bandwidth and security across your entire infrastructure.
1.800.800.0014 ■ www.connection.com/RUCKUS

COMMSCOPE®