Introduction to AuthPoint

WatchGuard Training

What is AuthPoint?

- AuthPoint is a multi-factor authentication service available from WatchGuard Cloud
- AuthPoint authenticates users when they log in to a variety of applications
- You can choose different authentication methods for specific user groups and resources:
  - One-Time Password (OTP)
  - Push Notification
  - QR Code

AuthPoint Components

- AuthPoint management UI
  - Manage resources, groups, and users
  - Configure external identities and the AuthPoint Gateway
  - Download installers for the AuthPoint Gateway and Logon app
  - Set authentication settings
- AuthPoint Gateway
  - Lightweight software application installed on corporate network
  - Functions as a RADIUS server
  - Configure from the AuthPoint management UI

AuthPoint Components

- Logon app
  - Software application installed on computer or server
  - Enables you to require that users authenticate to log on
- AuthPoint mobile app
  - Used to authenticate when you get access to a corporate resource

AuthPoint Web UI

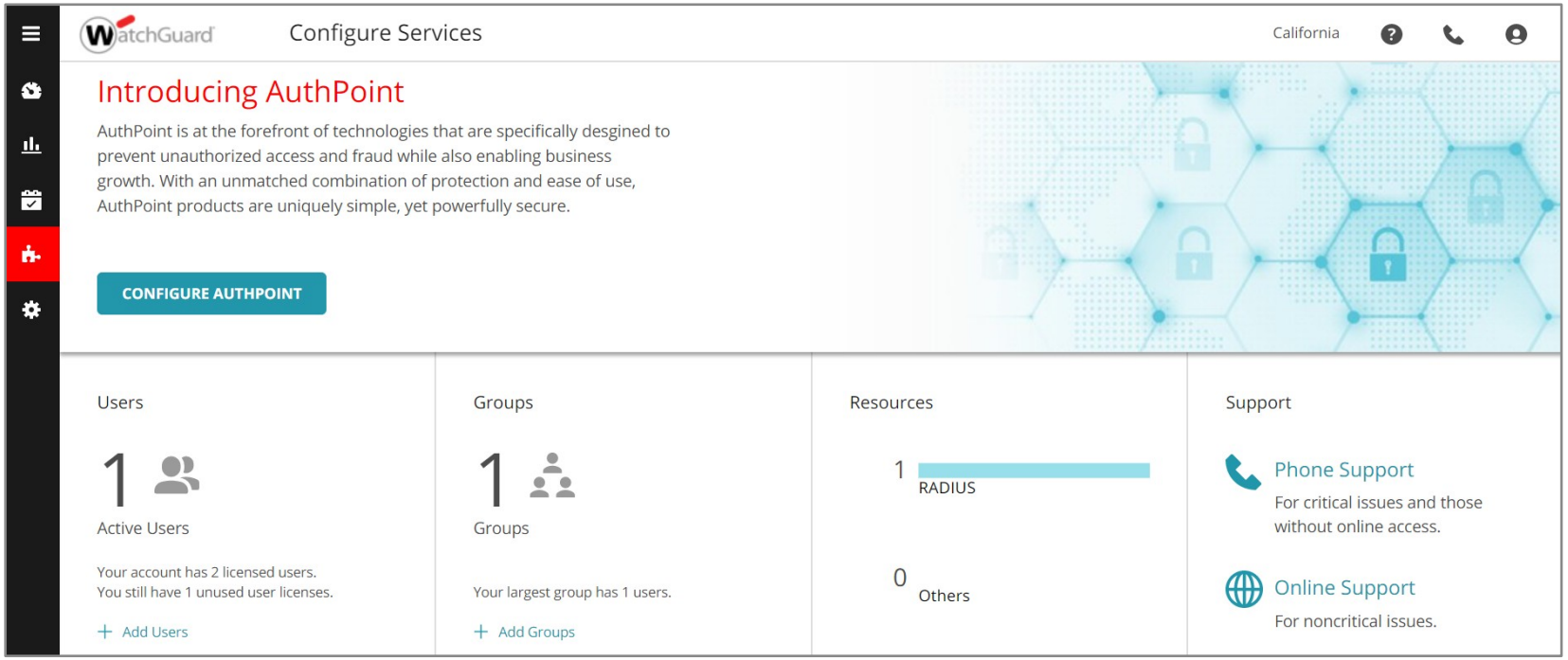
WatchGuard Training

AuthPoint Web UI

- Access the AuthPoint management UI from the **Configure Services** page in WatchGuard Cloud
- From the AuthPoint management UI, you set up and administer your AuthPoint deployment
  - Create and manage users and groups
  - Manage configurations for resources, external identities, and the AuthPoint Gateway
  - Download installers for the AuthPoint Gateway and Logon app
  - Set authentication settings

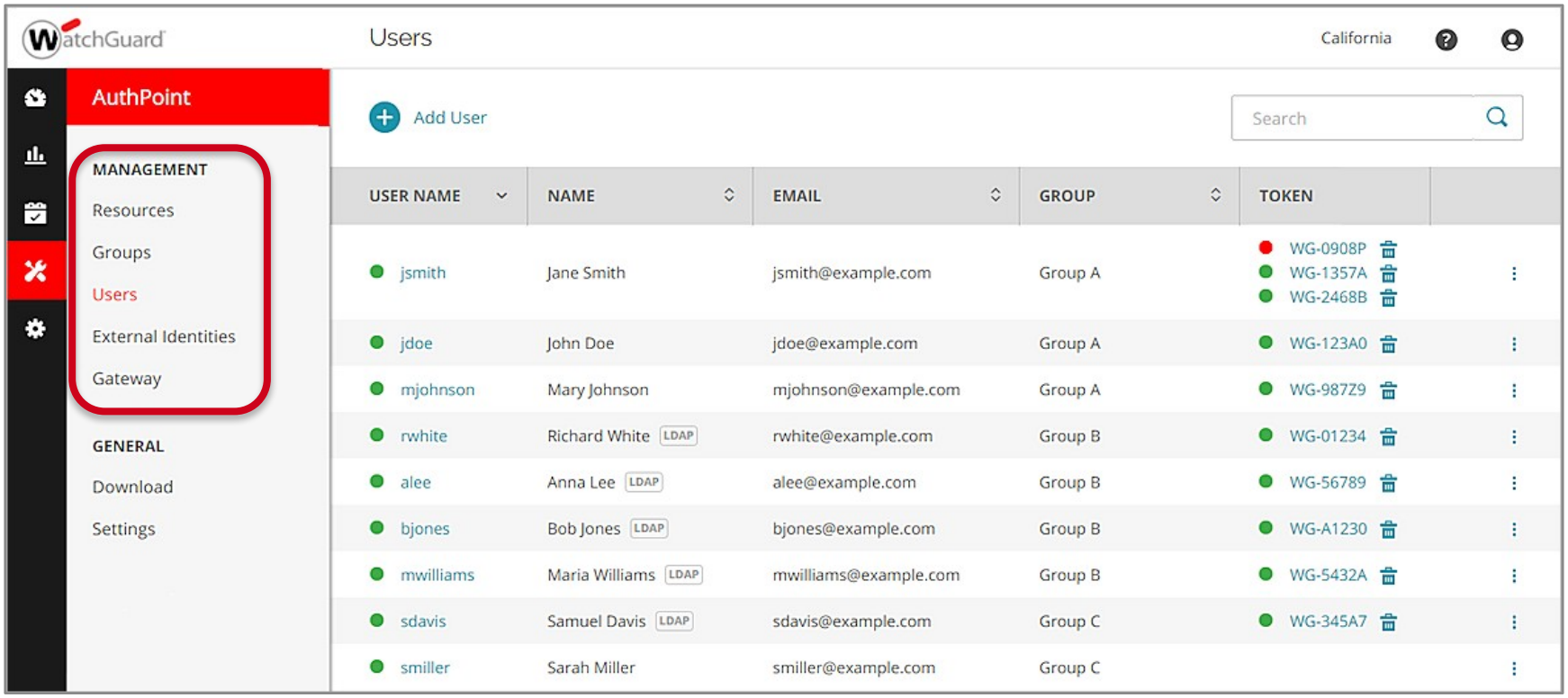
AuthPoint Web UI

- On the **Configure Services** page in WatchGuard Cloud, you can see an overview of your users, groups, and resources
- Click **Configure AuthPoint** to open the AuthPoint web UI



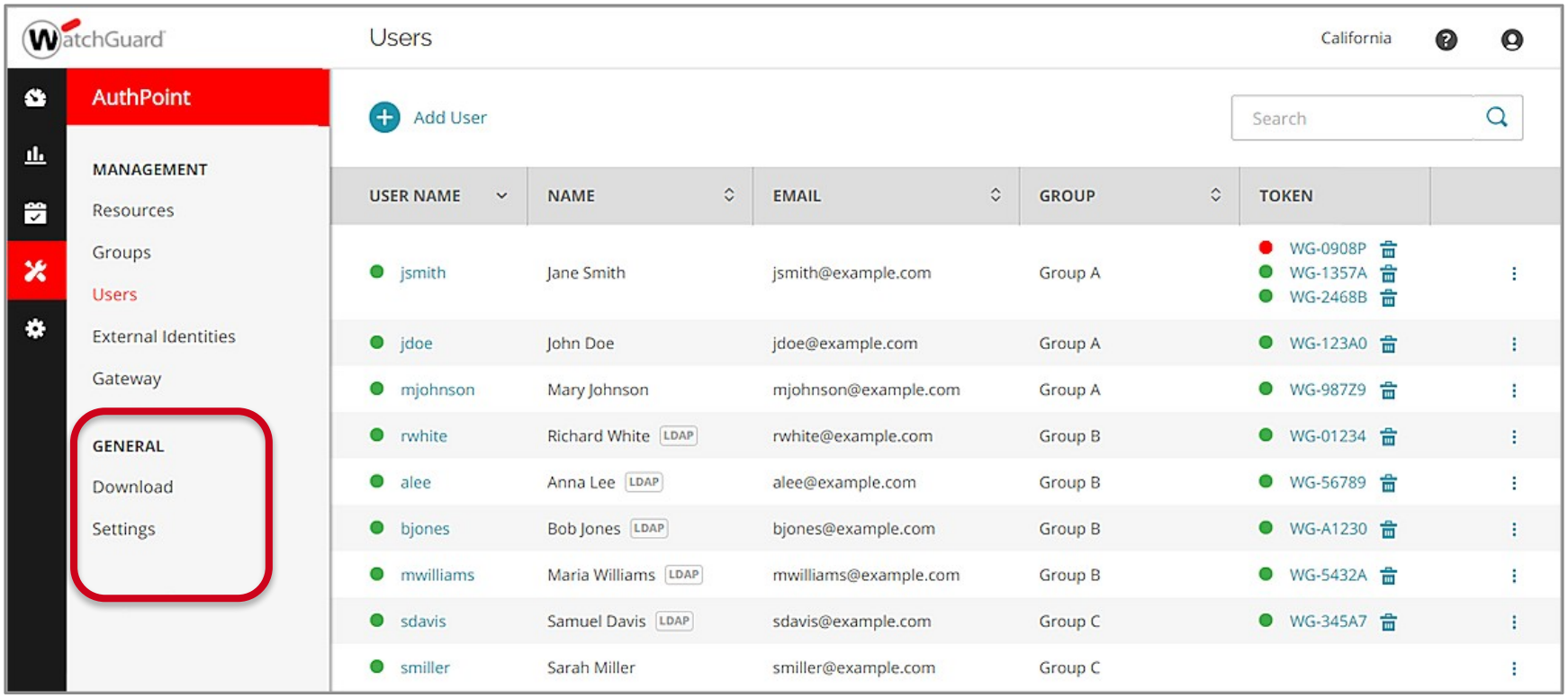
AuthPoint Web UI

- From the **Management** menu, you can get access to the Resources, Groups, Users, External Identities, and Gateway pages



AuthPoint Web UI

- From the **General** menu, you can get access to the Download and Settings pages



AuthPoint Management

- **Resources** — The applications that you define for use with AuthPoint
- **Groups** — Create groups of users and assign access policies to the group
- **Users** — View and manage your user accounts
- **External identities** — Connect to user databases to get user account information and validate passwords
- **Gateway** — For LDAP and RADIUS integration

AuthPoint General

- **Download** — A page where you download the installers for the Gateway and Logon app
- **Settings** — Where you define authentication settings

About Resources

- A resource is an application or service that you want to connect to, combined with the information required to connect to that resource
- Resource types:
  - RADIUS Client
  - SAML
  - IdP Portal (The Identity Provider (IdP) portal resource is a portal page that shows users a list of SAML resources available to them.)
  - Logon App
  - Firebox
  - ADFS
  - RD Web (Windows Server with the Remote Desktop Web Access Role configured)

AuthPoint integration

https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/_intro/authpoint-integrations.html

- M-Files Integration with AuthPoint
- Malwarebytes Nebula Integration with AuthPoint
- ManageEngine Desktop Central Integration with AuthPoint
- ManageEngine PMP Integration with AuthPoint
- Microsoft Intune Integration with AuthPoint Logon App for Windows
- MobileIron Integration with AuthPoint
- Moodle Integration with AuthPoint
- NetDocuments Integration with AuthPoint
- NetIQ eDirectory Integration with AuthPoint
- New Relic Integration with AuthPoint
- Nextcloud Integration with AuthPoint
- Microsoft 365 Integration with AuthPoint
- OneLogin Integration with AuthPoint
- OpenVPN Access Server Integration with AuthPoint
- OpsGenie Integration with AuthPoint
- Oracle Identity Cloud Service Integration with AuthPoint
- PagerDuty Integration with AuthPoint
- PagerTree Integration with AuthPoint
- Palo Alto Networks GlobalProtect Integration with AuthPoint
- Parallels RAS Integration with AuthPoint
- Perforce Integration with AuthPoint
- pfSense OpenVPN Integration with AuthPoint
- Pipedrive Integration with AuthPoint
- Planview ProjectPlace Integration with AuthPoint
- Pleasant Password Server Integration with AuthPoint

About RADIUS Client Resources

- RADIUS client resources represent RADIUS clients
- RADIUS client resource type is used most commonly for firewalls (primarily for VPNs)
- The AuthPoint Gateway functions as the RADIUS server
- RADIUS client resources must have a shared secret so the RADIUS server (AuthPoint Gateway) and the RADIUS client can communicate
- RADIUS client resources must be linked to a Gateway in the AuthPoint web UI

About SAML Resources

- SAML is a method for exchanging information between a service provider and an identity provider
  - Service provider — The provider of a third-party service that users connect to, such as Salesforce or Office 365
  - Identity provider — AuthPoint
- In AuthPoint, SAML resources connect AuthPoint with a service provider to make users authenticate before they can connect to that service or application

About IdP Portal Resources

- The Identity Provider (IdP) portal resource is a portal page that shows users a list of SAML resources available to them
- When you add an access policy for an Identity Provider (IdP) Portal to a group, users that are part of that group will see the portal page
- Only for SAML resources
- One IdP Portal resource can be used for all groups

About the Logon App Resource

- The Logon app resource is how you configure and define access policies for the Logon app
- When you add an access policy for the Logon app resource to a group, any user that is part of that group must authenticate to log on to any computer or server where the Logon app is installed

About Groups

- Groups are assigned access policies to specify which resources require authentication and which authentication method to use (OTP, Push, QR code)
- You must add at least one group before you can add users
- Users can only be in one group

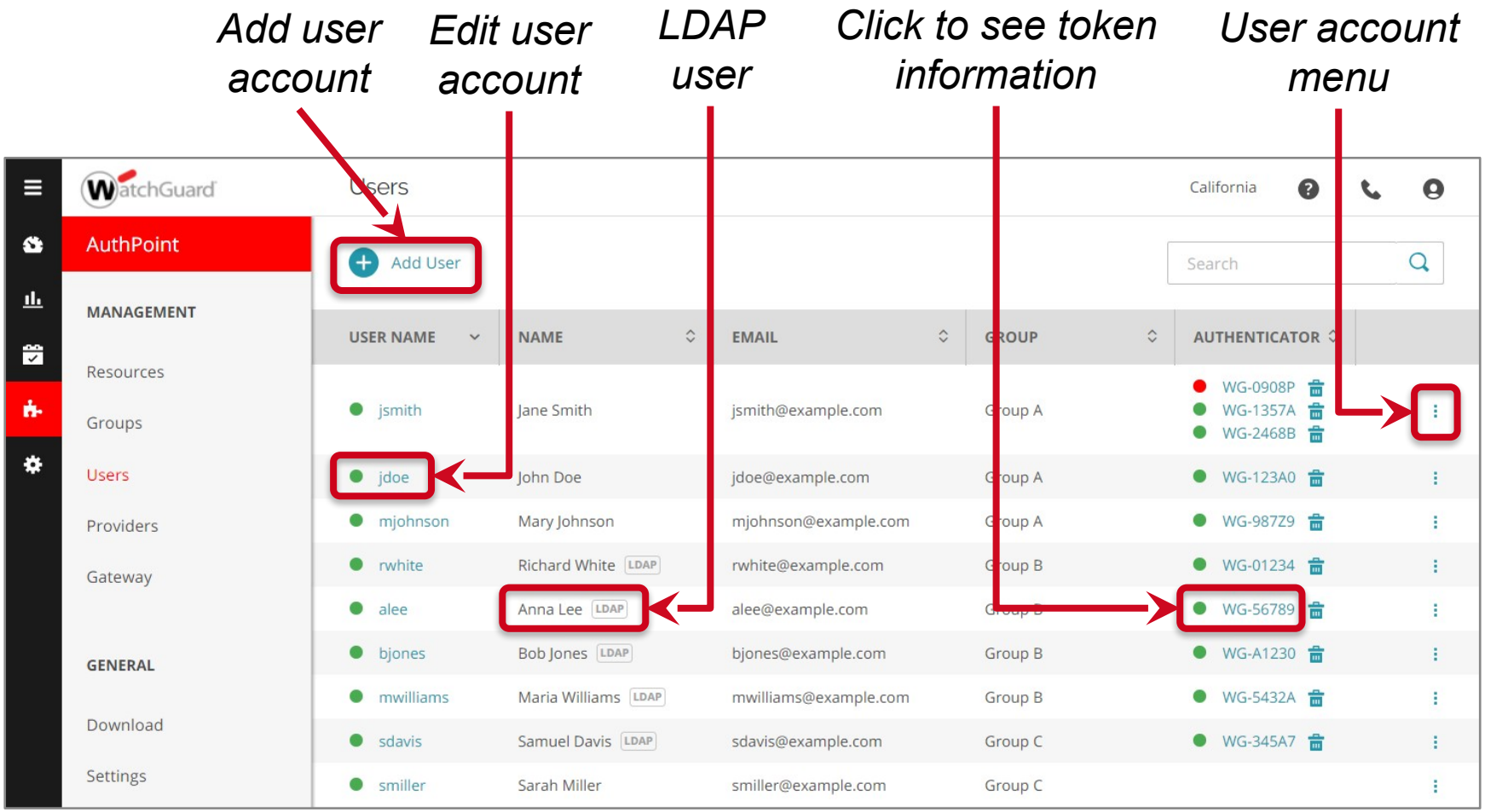
Access Policies

- For each user group, assign access policies to specify the resources that require authentication, and the authentication method for each resource (OTP, Push, QR code)
- You can add access policies when you create a group or you can add access policies to a group that already exists

Manage User Accounts

- On the **Users** page, you can see all AuthPoint user accounts and the details for each account
- You can:
  - Add, edit, block, unblock, and delete user accounts
  - See the status of a user account
  - Identify LDAP users
  - See token information for a user account
  - See and change the token status
  - Send the activation email again
  - Send the set password email again
  - Delete the token for a user account

Manage User Accounts



Manage User Accounts

- To add AuthPoint user accounts, choose a method:
  - Manually — On the **Users** page, click **Add**
  - Automatically — Specify an LDAP provider database where user accounts are stored and can be synced with AuthPoint
- Each user account:
  - Must be assigned to a group
  - Can only be included in one group
  - Must have a unique user name and email address

About External Identities

- External identities interact with external user databases to get user information and validate passwords
- On the **External Identities** page, you can configure the settings for connections to your LDAP server
- AuthPoint sends queries to your LDAP database to get user account information for authentication with AuthPoint
  - The AuthPoint Gateway must be installed in the environment
  - You can run a query to add LDAP user accounts to AuthPoint
  - When you change user account information in your LDAP server, it is automatically updated in AuthPoint when a sync occurs
  - You can manually initiate a sync of user accounts

Logon App

WatchGuard Training

About the Logon App

- The Logon app is used to require authentication when users log on to a computer or server
- There are two parts to the Logon app:
  - The application you install
  - The resource you add in AuthPoint
- Add a Logon app resource in the AuthPoint web UI, then install the Logon app (with a configuration file) on each computer or server that you want to protect
- When the Logon app is installed and an access policy is defined for the resource, users must authenticate to log on to the computer
- Download the Logon app installer on the **Download** page

AuthPoint Gateways

WatchGuard Training

About Gateways

- Gateways are a lightweight software application that you install on your network to synchronize user account information between your LDAP or Active Directory server and AuthPoint
  - Configure the Gateway in the AuthPoint web UI
  - Download the Gateway installer on the **Download** page
- A Gateway is required for RADIUS authentication
- A Gateway is required for LDAP synced users to authenticate with SAML resources
- The Gateway functions as a RADIUS server

AuthPoint Mobile App

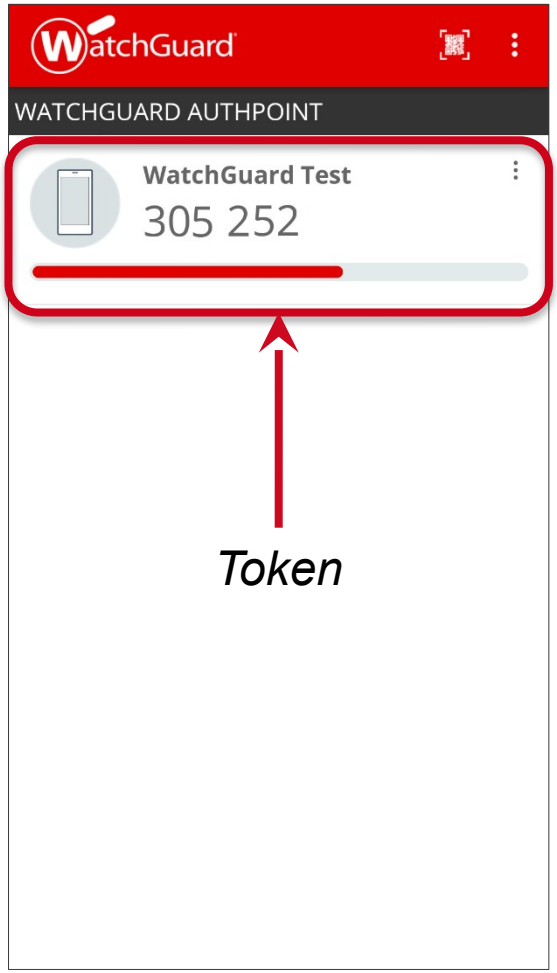
WatchGuard Training

AuthPoint Mobile App

- With the AuthPoint mobile app and a token, you have everything you need to authenticate
- The app is where you see and manage your tokens
- Device DNA adds security
- PIN protection for your tokens adds an extra layer of security

AuthPoint Mobile App

- Before you can authenticate with AuthPoint, you must install the AuthPoint app on your mobile device
- The app shows all of your active tokens and enables authentication with these methods:
  - Push Notification
  - One-Time Password (OTP)
  - QR Code
- You can edit the name and image for each token
- The app includes a QR code reader



Authentication

- When you try to connect to a resource that requires authentication, you are redirected to the AuthPoint SSO page
- The AuthPoint app enables authentication with these methods:
  - Push notification
  - One-time password
  - QR code
- Some resources may require specific authentication methods or only have certain methods available
- The authentication methods available on the SSO page are based on the access policies assigned to your user group

AuthPoint in WatchGuard Cloud

WatchGuard Training

What is WatchGuard Cloud

- WatchGuard Cloud allows you to see and manage all of your products and services in one place
  - Dashboard shows a summary of aggregated information to give you a quick overview of your account
  - Reports show you information about your configured security services
  - The **Configure Services** page is where you configure security services such as AuthPoint
- There are two types of accounts in WatchGuard Cloud:
  - Subscriber
  - Service Provider