Wi-Fi Connection

Remote device permission policies can be configured for public Wi-Fi connectivity. These policies allow you to block access to public Wi-Fi networks for specific devices or groups of devices. Policies can be applied to Windows and macOS devices.

Public Wi-Fi networks

Public Wi-Fi networks, found in places like coffee shops, airports, and hotels offer convenient internet access for users on the go. However, they come with significant security vulnerabilities. Connecting to public Wi-Fi can expose your sensitive data to potential threats as these networks are often unsecured and easily targeted by cybercriminals. It's crucial to exercise caution and take appropriate measures to protect your privacy and security when using public Wi-Fi.

Blocking public Wi-Fi access on a device provides the following benefits:

- Enhanced security
- Protection for data privacy
- Minimize exposure to threats

Wi-Fi connectivity policies

Coro offers two Wi-Fi connectivity policies:

1. **Allow connection to all encrypting networks**: Blocks access to all public Wi-Fi networks, and only allows access to WPA+ (WPA and higher) networks.
2. **Allow connection to specific connections**: Blocks access to all public Wi-Fi networks. Only networks with specific SSIDs (the unique names assigned to wireless networks) are allowed.

> **Note**
>
> If no policy is applied to a device, that device has no restrictions on Wi-Fi connectivity.

Configuring Wi-Fi connectivity policies

To configure a new public Wi-Fi blocking policy:

1. From the **Device Posture** tab, select **+ ADD**.