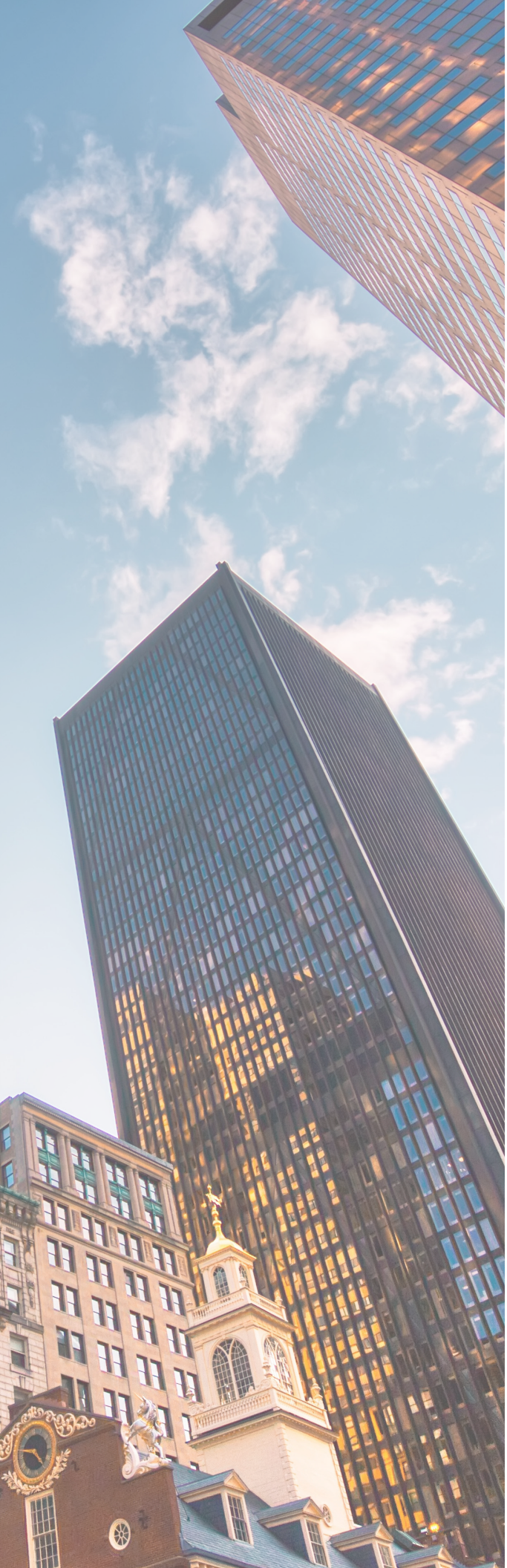
NOMADIX®

Implications of MAC Randomization or ‘Private Address’ for your Property and Guests



BACKGROUND

Nomadix co-founder, Dr. Leonard Kleinrock, recognized as one of the inventors of the Internet, developed what is known as today's visitor-based network (VBN). Visitor-based networks are encountered when guests access the Internet at hotels, temporary environments like Starbucks or any location where a guest is trying to access Wi-Fi.

One of the enabling technologies behind these visitor-based networks are Nomadix gateways. A key capability Nomadix gateways provide is to manage all the devices connected to a visitor-based network in regards to allowing access, enabling appropriate guest entitlements such as bandwidth upgrades and the total number of devices that are allowed to connect to the network.

Guest devices are identified by using the Media Access Control (MAC) address of each guest device. A MAC address is a unique identifier associated with specific network hardware on a device. This use of the MAC address enables the identification, management and authentication of individual devices wherever it connects or moves around the network. This management and control was defined and designed when the VBN was created by Dr. Kleinrock.

Today this Nomadix technology facilitates many millions of connections daily. Public venues rely on Nomadix's bandwidth management and authentication technology to control, customize and optimize users' internet access and user experience 24/7.

WHAT IS CHANGING?

Mobile devices, including phones, tablets and laptops, have come a long way since the introduction of the VBN. Devices are being updated to be more secure in regards to Personally Identifiable Information (PII), network traffic and the ability to be tracked.

One security solution that has been rolled out by device manufacturers like Google, Apple and others is to use a new, random MAC address each time a device communicates with a new wireless network. Once connected to that wireless network, devices utilize a set MAC address each time a connection is made to that network.

The latest announcement for iOS 14, which is expected to ship in September 2020, stated that Apple is changing the way that MAC addresses are assigned when devices remain connected to

a wireless network for an extended duration, for example, more than a day. This randomization of assigned MAC addresses, called Private Addresses, ensures that devices can't be tracked or profiled as they roam across multiple Wi-Fi networks or remain on a single Wi-Fi network for a sustained period of time. From Apple's announcement:

> *"If the device always uses the same Wi-Fi MAC address, network operators and other network observers can more easily relate that address to the device's network activity and location over time. This allows a kind of user tracking or profiling, and it applies to all devices on all Wi-Fi networks. To reduce this privacy risk, iOS 14, iPadOS 14, and watchOS 7 include a feature that periodically changes the MAC address your device uses with each Wi-Fi network."*

In addition, Apple has stated that the MAC address of a mobile device may be changed as frequently as every 24 hours, even when connected to the same network. However, a MAC address will not be changed while there is an active connection to avoid interrupting activities such as video streaming and other extended connections.

WHAT DOES THIS MEAN FOR PROPERTIES AND GUESTS?

Guests and properties will see various impacts from the increased frequency of randomization of the MAC address.

Visitor-based networks usually require some form of authentication, or at least acceptance of terms and conditions. In many cases, the MAC address is currently used as the unique identifier for a device. This change by Apple iOS14 means that the MAC address is not a reliable identifier to manage device sessions or grant guest entitlements such as upgraded bandwidth that extend beyond 24 hours.

In addition, reports or limits, for example the number of devices that can connect from each room, that rely on the MAC address may no longer be accurate as a single device can connect with several different MAC addresses.

Some brands and hotels utilize the MAC address to recognize devices of loyalty or VIP guests. Other authentication methods will be needed to identify these guests.

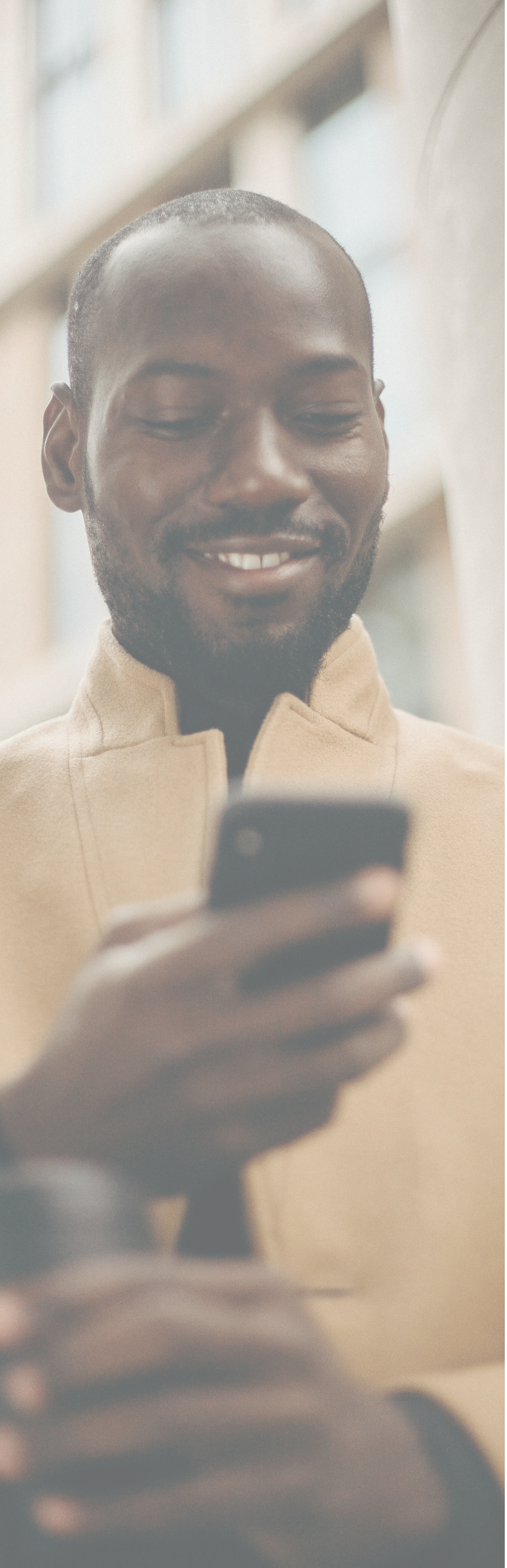
WHAT ARE THE OPTIONS?

There are several options to eliminate or minimize the impact of MAC randomization on guests:

- Implement HotSpot 2.0, also known as Passpoint
- Enable alternative authentication methods
- Modify internet service offerings
- Ask guests to turn off the Apple Private Address feature

Each option provides various benefits and trade-offs for properties and guests.

	HotSpot 2.0 Enabled	Alternative Authentication Methods Enabled	Modify Internet Service Offerings With 24 Hour Limit	Request Guests Disable Private Addresses
Present Property Portal for Initial Connection	YES	YES	YES	YES
Require Guests to Authenticate Again After 24 Hours	NO	YES	YES	NO
Retain All Guest Entitlements After 24 Hours	YES	YES	NO	YES
Enable Automatic VIP Access	YES	NO	NO	YES
Guest Experience	A+	A	B	C
Guest Devices Supported	Most	All	All	Some



HotSpot 2.0

Currently the best option for a different identifier is to implement Hotspot 2.0, also known as Passpoint, on any device that can support it. Having a Hotspot 2.0 profile on the device and enabled on the wireless network at the VBN site allows for seamless authentication and management of the network and decouples the identity of the device from the MAC address which can no longer be counted on to remain static during a guest's stay.

HotSpot 2.0 is an authentication method where a profile associated with a property's wireless network is installed on a guest's device so authentication doesn't rely on the MAC address and automatically triggers authentication on that wireless network.

To utilize HotSpot 2.0, a profile must be installed on the guest device and enabled at the property. Nomadix can enable HotSpot on Nomadix managed networks through our partnership with GlobalReach Technology, (globalreachtech.com) a proven leader in Hotspot 2.0 implementation and delivery. The Nomadix Mobile Guest application or mobile app HotSpot 2.0 SDK can help facilitate the installation of a HotSpot 2.0 profile.

Hostpot 2.0 is supported by most current devices and VBNs and is growing to be nearly universal. However, in the few cases where older, incompatible devices or networks are not supported, other options would need to be explored.

Alternative Methods of Authentication

Implementing alternative methods of authentication allows internet access purchases and entitlements such as loyalty program benefits and bandwidth upgrades to persist for guest stays longer than 24 hours. With guest authentication, the new MAC address associated with the device can also be associated with the guest and the appropriate access privileges enabled.

Examples of potential authentication options include Vouchers, PMS, or other authentication that is tied to an entry, like a username password pair, that the guest can enter for all the different devices or device identities when the MAC address changes. In this scenario, there can be no limit to the number of devices that can be linked to the authentication.

With this option, guests may still need to authenticate every 24 hours. However, loyalty program benefits, bandwidth upgrades and other entitlements would be maintained over the entire duration of a guest stay. All devices would be supported with this approach.

Modify Internet Service Offerings

Setting guest expectations that authentication will be required every 24 hours, modifying offered internet service options to have durations of 24 hours and disabling per room device limits is another option for guests using affected Apple devices.

For any Guest Network authentication plans that charge for the access, set the duration time to less than 24 hours. This will still require affected devices to re-authenticate; however, this avoids refunding guests who might otherwise purchase Wi-Fi connection packages longer than 24 hours. Per room limits on the number of devices that can attend should also be disabled so guests do not receive messages saying the maximum number of devices have connected when it's actually the same device with a changed MAC address.

For any free access Guest authentication plans that require an acceptance of Terms and Conditions, the duration should also be set to less than 24 hours.

Modifying the terms of the internet service offerings would still require guests to authenticate every 24 hours. In addition, loyalty program benefits, bandwidth upgrades and other entitlements would not be maintained longer than 24 hours.

Turn Off the Private Address Feature

Guests and employee devices running Apple iOS 14 or above have the option of disabling the Private Address feature for the site's specific wireless network. With this feature turned off, MAC addresses of guest and employee devices would not change over the duration of the connection. This consistent MAC address would allow access to the wireless network for as long as the authentication permits.

However, this approach would likely require a call to the front desk or support. In addition, guests may have concerns about the security implications of disabling this feature. These concerns are amplified by the security warning that appears on a guest device with this feature disabled. Because it is unclear how many guests with Apple devices would agree to turning off this feature, this option cannot be counted on to provide a solution for all guests.

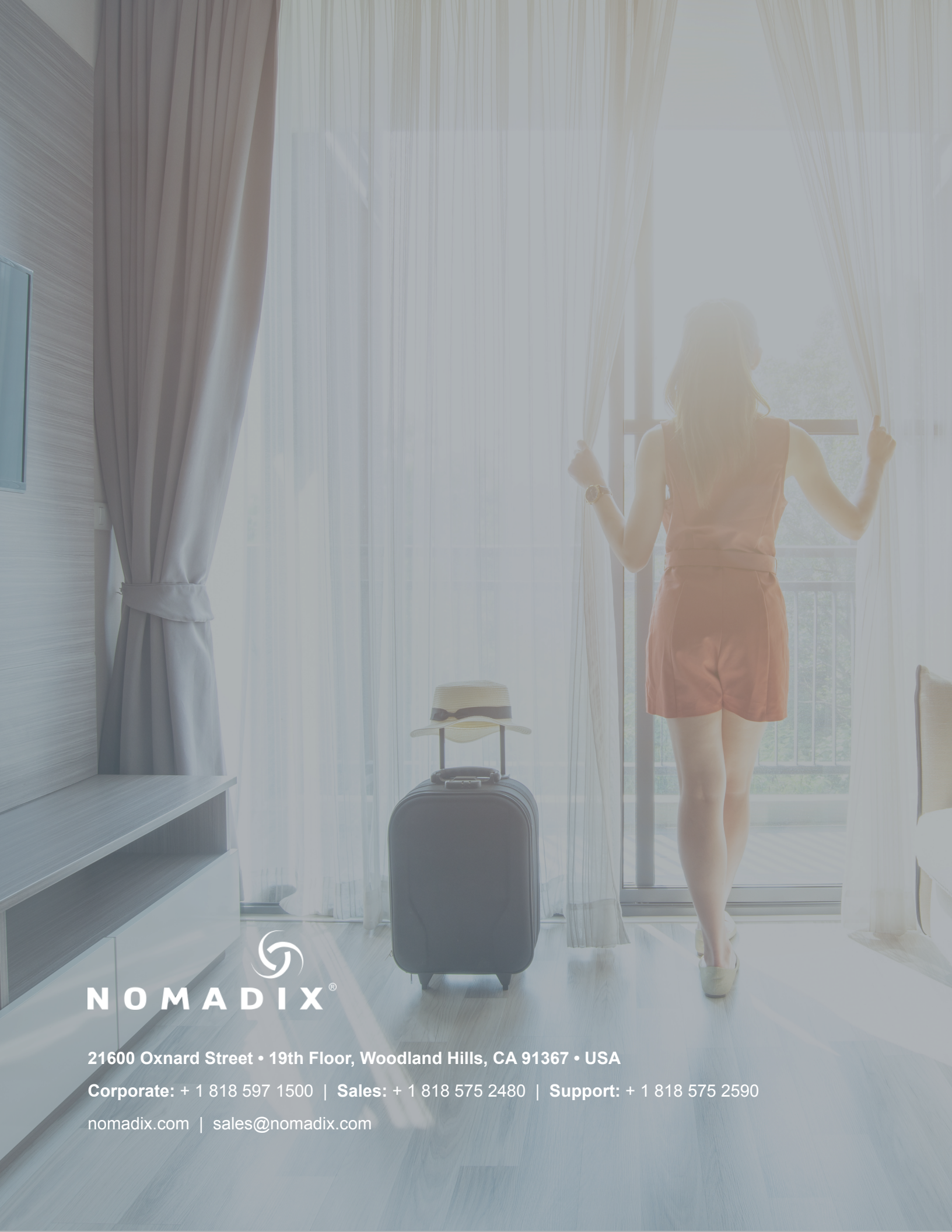
Detailed instructions on how to turn Private Addresses off or on for a wireless network can be found on Apple's support site. A summary for iPhones, iPads and iPods running iOS14 is on the next page.

You can stop or resume using Private Addresses on an iPhone, iPad, or iPod touch running iOS 14:

1. Open the Settings app, then tap Wi-Fi.
2. Tap the information button ⓘ next to a network.
3. Tap Use Private Address. If your device joined the network without using a private address, a privacy warning explains why.
4. The new setting is used the next time your device joins the network. If you want to use it immediately, turn Wi-Fi off and back on in Control Center or Settings, then join the network.

NEXT STEPS

Nomadix is here to help you navigate this important change. We welcome the opportunity to discuss the best option for your property. Please call your sales or support team to help identify the best solution for your employees and guests.



NOMADIX®

21600 Oxnard Street • 19th Floor, Woodland Hills, CA 91367 • USA

Corporate: + 1 818 597 1500 | **Sales:** + 1 818 575 2480 | **Support:** + 1 818 575 2590

nomadix.com | sales@nomadix.com