Phonism

Security White-paper

Introduction

Phonism is a cloud-based solution for managing and provisioning VoIP devices. In this paper, we discuss the problems around managing and provisioning VoIP devices and how Phonism addresses security concerns when managing and provisioning these devices.

Security Concerns in VoIP Device Market

A lot of existing solutions in the marketplace still serve configuration files to devices in cleartext and over insecure protocols like TFTP. TFTP has historically been a standard protocol for devices to use to communicate with a provisioning and configuration server. This protocol sends cleartext data over UDP and should never be used over the cloud. Using TFTP over a VPN tunnel may suffice but should not be recommended for commercial applications.

A lot of the security concerns in the VoIP device market exist because of the large amount of legacy devices still in use and the insecure protocols that they support. Some VoIP phones in the marketplace today still only support provisioning over TFTP.

Furthermore, many provisioning servers on the market simply serve configuration files from a single directory containing all files pertaining to a customers' phones. These servers are typically FTP or HTTP servers. The problem with using a simple FTP or HTTP server is that requests are not authorized, opening the server up to easily scripted attacks.

Phonism supports HTTPS which is the default protocol support for all devices in the system and we encourage our customers to use HTTPS as well. Phonism authorizes every request sent by devices to prevent unauthorized access to configuration data.

Phonism

How does Phonism address these concerns?

Encryption

All traffic through our system is encrypted with SSL/TLS. VoIP devices utilizing Phonism for management and provisioning communicate via HTTPS.

Authentication

Phonism also provides the ability to setup device authentication allowing administrators to configure provisioning credentials for their devices. For example: When a group of VoIP phones are installed at a customer location, administrators can set up that location in Phonism as a tenant and also configure tenant authentication. This enables authentication for all phones at that customer location. Once enabled, all configuration requests from those phones are authenticated using the HTTP authentication methods supported by the phones themselves.

Authorization of devices

Whenever a request is received by a VoIP device, after authentication has occurred, Phonism authorizes the request by MAC address, brand, and device model. For example: If a request is received from an unknown MAC address, the request is denied. If a request is received for a MAC address, but does not match the original model of the device, it is denied as well. The same goes for brand of the device.

Whitelist IP addresses

It is also possible to enter a list of IP addresses for each tenant site that will authorize devices (with the proper mac addresses) to get the provisioning, firmware and configuration information, without needing to add tenant credentials. In some cases, certain manufacturers do not allow the administrative credentials to be added (some MItel phones for example), and entering a whitelist IP address still allows for authentication of the site.

Data Storage & Compliance

Phonism protects and secures all data in the database using AWS-256 encryption. Phonism is compliant with European data laws - GDRP - General Data Protection Regulation.

Ready to reinvent the way you onboard and provision your phones?

Learn more at
phonism.com/get-started