COMMS
COUNCIL
UK

THE VOICE OF ADVANCED COMMUNICATIONS

Comms Council UK's

Recommendations for Device Provisioning Security

Version 3

January 2025

Contact: team@commscouncil.uk

Contents

Summary

- Remote provisioning delivers substantial benefits for ITSPs & End Users
- Provisioning servers are a prime target for attack and must be secured effectively
- Authenticate provisioning using HTTPS factory installed client certificates.
- Ensure that security is maintained at every point in the provisioning process.
- Do not use TFTP, HTTP, FTP or unencrypted protocols for remote provisioning.
- Delete SIP passwords from SIP servers as soon as provisioned, if possible.

Introduction

The ability for ITSPs to remotely provision phones & other SIP devices greatly improves service delivery, customer experience and is essential to ensure the overall security of a device. A complete provisioning server set-up can deliver firmware security updates, automate the changing of passwords for accounts and even help with the rollout of new services. However, provisioning servers provide a focal point for hackers to steal account details and SIP credentials that can lead to serious security breaches if not secured thoroughly.

Many SIP phones have a mechanism for automating the configuration of their settings via remote network provisioning servers. This document provides an overview of the automatic provisioning methods used by most the devices and explains the role of Zero Touch Provisioning (ZTP) for an end to end manufacturer to service provider provisioning process.

There are many challenges to securing provisioning servers due to the variety of provisioning implementations provided by phone manufacturers. The aim of this document is to share Best Common Practices among CCUK members to help them secure their provisioning infrastructure. These recommendations should be considered a starting point rather than a complete solution as much will depend on the ITSP's choice of phone manufacturer and the type of service they operate.

By "Provision" we mean fully automated remote configuration and subsequent management of SIP phones. This is relevant to many SIP User Agents, Handsets, Gateways, ATAs or Softphones.

Risks

Poorly secured or badly implemented provisioning servers lead to SIP username and passwords being exposed to the world. There are many attack vectors and weaknesses that can lead to compromised provisioning servers.

1. It is simple to predict the MAC addresses of phones and scan servers.
2. It is possible to locate actual provisioning servers by following the redirections from manufacturer’s zero touch systems.
3. Differences in manufacturer provisioning implementations make securing servers a considerable challenge.

Unfortunately, some ITSPs have been found to be placing provisioning files on open webservers with no authentication, and have been surprised when their customers’ SIP credentials were harvested and used to make fraudulent calls. The good news is that when Remote Provisioning is sensibly secured the risks are minimal to all concerned.

Automatic Provisioning Methods

Phones can be remotely provisioned using a variety of communications protocols, each with different levels of security.

Provisioning Communications Protocols

Protocol	Encryption	Security Level	Recommendation
TFTP	NONE	POOR	Do not use, except within a secure network
HTTP	NONE	LOW	Avoid if better available
FTP	NONE	LOW	Avoid if better available
HTTPS without factory installed certificates	SSL	GOOD	Use together with usernames and passwords per device
HTTPS with factory installed client certificates	SSL	BEST AVAILABLE	Use with client certificate validation enabled on server.

Using an encrypted protocol for provisioning, at the highest level possible, is essential to prevent the intercept of account details by network sniffers or surveillance equipment.

The use of TFTP should be avoided at all costs since this protocol cannot be secured with usernames/passwords, is not encrypted and is a known target for viruses and scanners.

HTTP and FTP should not be used if HTTPS is available. ITSPs need to quantify the risks of operating with HTTP and FTP if there is no alternative and design a process that reduces the risk. We do not know of any device that supports HTTP and not HTTPs.

HTTPs should be secured by taking advantage of factory installed client certificates and using the highest level of cipher and protocol version possible. TLS 1.0 and 1.1 are widely recognised as being insecure. Where possible TLS 1.2 must be used without the ability to downgrade negotiation to older versions. Many devices are limited to SHA1 certificates, weak protocol versions and weak ciphers that are not recommended for use anymore. This ultimately produces a challenge for ITSPs and should be considered carefully to reduce risks. Best practice would be to operate at the highest level of security provided by a phone and avoid reducing the overall provisioning server security level to the capabilities of older models.

Encrypting Provisioning Configuration Files

Some manufacturers have included the support the encryption of configuration file content. This addition to the provisioning process provides an extra level of protection for provisioning servers and for the overall provisioning process.

HTTPS with client certificate authentication

HTTPS client certificates provide an excellent way to authenticate provisioning as the Provisioning server can cryptographically verify the identity of the phone. Factory installed certificates provide strong identity and should be used when available. This is the CCUK recommended way to authenticate provisioning requests.

The key benefits of factory installed HTTPs client certificates are

1. Strong identity removes ability for attacker to scan or fake requests.
2. Simple to implement with freely available open source and commercial web servers.
3. MAC addresses cannot be faked since certificate contains trusted MAC data.

The security model does rely on the manufacturer securing their certificate issuing process at the factory and securely storing the top-level CA certificate keys to prevent any unauthorised certificates being made.

Note that some manufacturers introduced factory client certificates after the initial production of devices. This has led to some models being available with and without factory certificates. It is a challenge for an ITSP to distinguish these devices and a best effort approach should be taken.

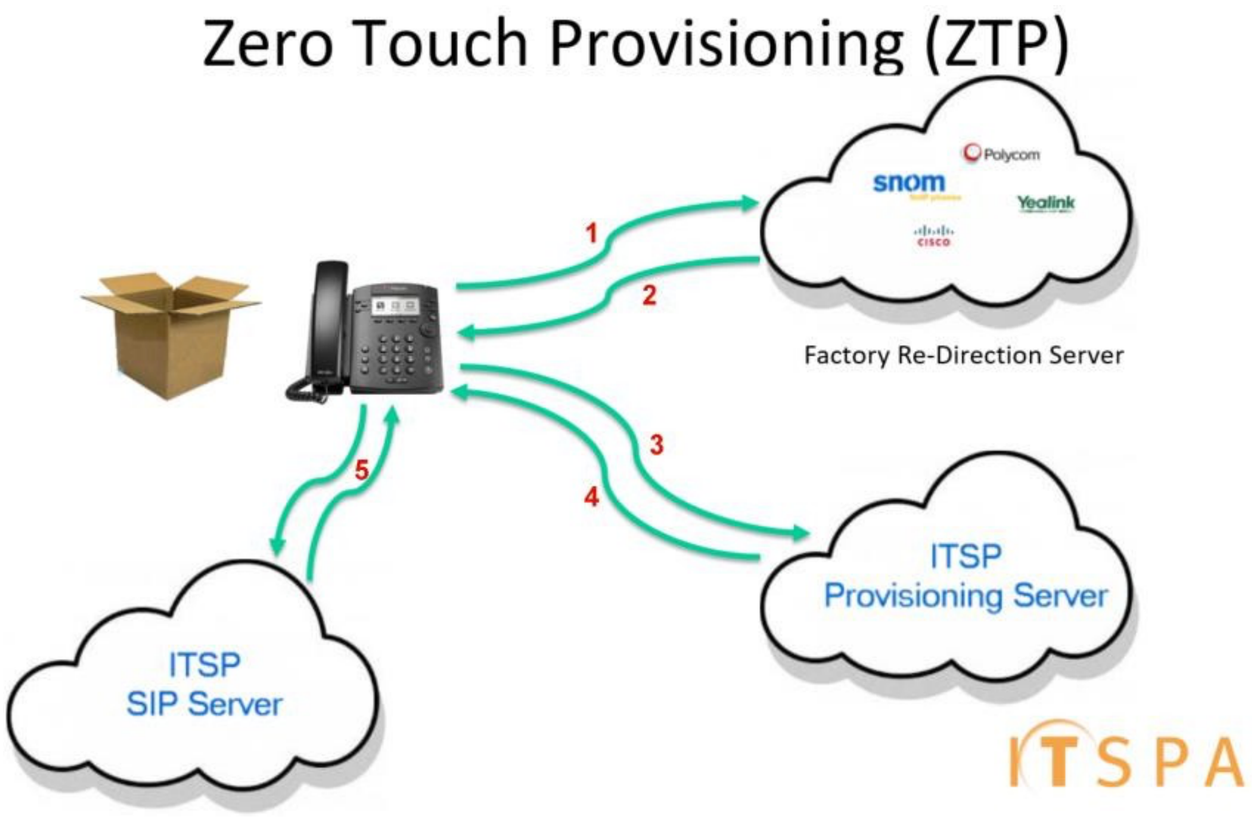
TFTP should only be used in a secure controlled environment

TFTP is used by many phones to locate their initial boot configuration, typically for providing the location of the actual provisioning servers and often only on the first activation of a device by an ITSP or equipment wholesaler to set a secure provisioning server address. This use of TFTP should be limited to the initial configuration of a device and should be in a secure controlled environment if account credentials are installed. It is recommended that ITSPs do not use TFTP for the main provisioning of phones between themselves and customers.

There are many end user companies running their own TFTP provisioning servers on internal local networks independently of their ITSP. In these situations, we recommend that ITSPs advise customers based on the content of this document. It is not recommended that ITSPs supply services that require customers to operate their own provisioning servers reliant on TFTP.

Zero Touch Provisioning

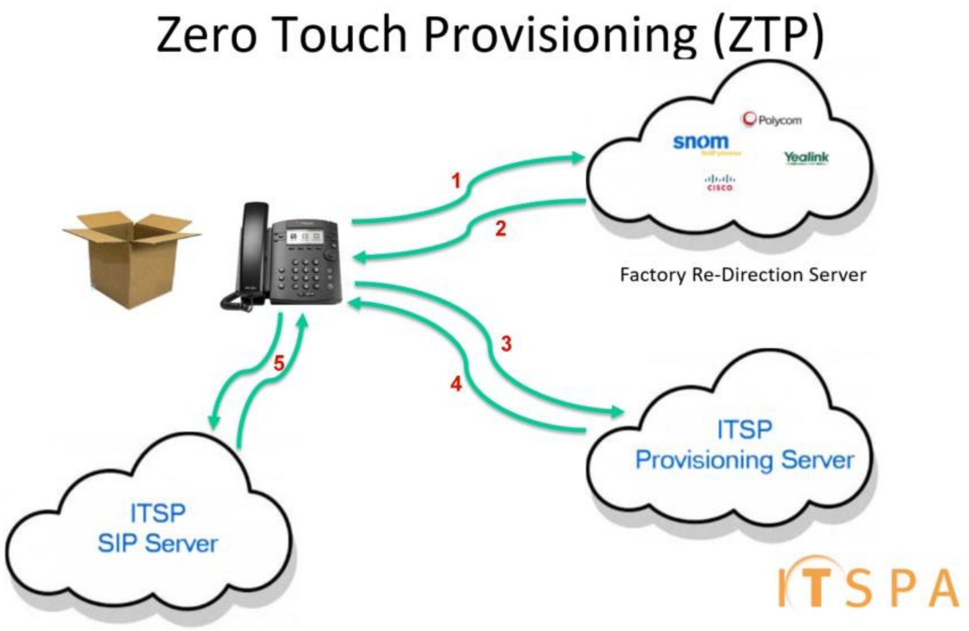
Zero Touch Provisioning (ZTP) is the process that enables the provisioning of phones from a manufacturer without needing to manually set-up the initial provisioning server details. This means that phones can be shipped direct to customers or at least boxes do not need to be opened to get them ready for customers. Service providers can register a phones MAC address with the phone manufacturers portal. When a phone first boots or after a factory reset, it connects to the manufacturers provisioning server and then redirects to the provisioning server of the ITSP to receive configuration and firmware updates.



In the Diagram above:

1. A new phone automatically contacts its Factory Re-Direction Server on first Boot.
2. If the phone's details have been listed, the redirection server responds with the relevant ITSP's Provisioning Server Details.
3. The phone contacts the ITSP's Provisioning Server.
4. The ITSP's Provisioning Server responds with the relevant SIP Credentials.
5. The phone contacts the ITSP's SIP / Provisioning Server and registers.

Zero Touch Provisioning Risks



ZTP Provisioning Weak Spots:

1. Step 1 & 2 are the responsibility of the manufacturer to secure. There is still a risk that their implementation is insecure.
2. Do not assume the manufacturer re-direction server will provide secure settings for your environment. For example, you may need to ensure the phones admin password is changed to a complex password before step 3 to avoid someone interrupting the provisioning process and viewing the ITSP Provisioning server details.
3. Steps 3, 4 & 5 must use HTTPS transport to avoid provisioning details being captured by a packet sniffer

- **Changing the phone's Admin Password before step 2 is often overlooked!**

Softphone Considerations

Softphones can be difficult to provision securely because most require SIP credentials to be entered manually or to use the manufacturers provisioning server. ITSPs should consider how they intend to handle and communicate account information for softphone users. Ideally, avoiding email as a delivery mechanism and instead providing a "reveal" mechanism from a web page secured by login.

Local SIP PBXs

Many SIP PBX systems include a provisioning server as part of the system. Installers should check carefully with how these are set-up and that it is protected from attack from the Internet and if possible restricted to any subnets where it is require. Again, security should be considered as part of the design and ensured at every stage of deployment since an attacker with local network access could still pose a threat where SIP credentials are easily accessible. As a best practice, we recommend that the same principles detailed in this document should apply to both service providers and Local SIP PBXs.

Third-Party Provisioning Servers

If you use either manufacturer ZTP servers or third party servers to provision your phones, then it is essential for you to check that the settings provided by them are secure. Some settings such as admin passwords and user accounts for access to web interfaces must be checked carefully to ensure are not left with defaults or shared across devices.

If you provision phones with a third-party operated provisioning server, you must ensure that you consider what the default settings are for key features such as logging and directories. Some models of phone upload directories and call lists to the provisioning server automatically. This will have a data protection impact with customer’s private data being stored outside areas of your control or governance.

Best Practice Recommendations:

1. ITSPs who deploy Remote Provisioning Servers must consider security as an integral part of the design.
2. Ensure that every step in the provisioning process is secure.
3. Change the phone’s Admin Password at the Factory Redirection Server.
4. Choose phone vendors who have a documented and audited authentication system for provisioning.
5. Where possible always use encrypted protocols and factory installed client certificates.
6. Use encrypted configuration files when supported by the device.
7. Keep provisioning server software up to date.
8. Firewall your provisioning server with rate limits to reduce impact of MAC address scans.
9. Review and monitor activity the logs for suspicious activity.
10. Regularly review security procedures and practices.
11. Automate the process of generating provisioning data on the ITSP provisioning server. The process should include an automated password generator set to generate mixed case alphanumeric passwords of 12 characters or more.

Provisioning Checklist

		Y/N
	Your Phone Manufacture’s Provisioning documentation has been reviewed and passed as secure.	
	Every leg of the provisioning process has been captured as a pcap, reviewed and confirmed as using https.	
	Check that you are using TLS 1.2 where possible with HTTPS communications.	
	Provisioning has been interrupted after the phone contacts the Factory re-direction server and you have confirmed that the default admin password has been changed.	
	You have captured a provisioned phone registering as a pcap, reviewed the process and confirmed that https is used throughout and that credentials are not being passed in plain text	
	You have scanned / Pen Tested your provisioning server for vulnerabilities	
	Ensure that you do **not**: • Deploy a Provisioning Server that uses TFTP, except on a secure network • Manually generate provisioning files	