# ALCATEL-LUCENT ENTERPRISE PROFESSIONAL SERVICES
## TOLL FRAUD PREVENTION

Identifying security gaps is an essential step in the fraud prevention process; ignoring them exposes enterprises to hazardous fraud that can cause serious harm. Bad debt, reputation and brand image loss, and legal conflicts are only some of the negative consequences that unaware organizations can experience.

The Toll Fraud Prevention Service reinforces enterprise protection against toll fraud. The service enables assessment of every installed Alcatel-Lucent Enterprise communication system, highlighting current vulnerabilities and potential threats, and providing advice to strengthen security and guidelines to prevent attacks.

### BENEFITS

- Proactively prevent fraud by identifying security gaps
- Pinpoint vulnerabilities to new threats, particularly for aging systems
- Ensure compliance with Alcatel-Lucent Enterprise security best practices

### SERVICE DESCRIPTION

The service starts by auditing the communication system in the customer premises. This audit focuses on solution security within the customer organization and ecosystem – how the system is used, operated and configured, and reviews the following areas:

- Access to the communication system (e.g., remote maintenance access)
- Embedded telephony protection mechanisms (e.g., external transfer protection)
- End-user rights (e.g., call barring)
- Configuration of telephony applications (e.g., voicemail application)
- IP security management (e.g., Secure Shell)
- History of operations (e.g., audit application)

Following the on-site audit, a Professional Services expert provides a detailed report containing both findings and recommendations. The report includes:

- An executive summary, which provides an overview of the solution's current vulnerabilities, including identified threats and associated impacts, and compliance with Alcatel-Lucent Enterprise security recommendations. The current situation may include – among other findings – information such as the top 10 called destinations, percentage of users with default and/or easy to find phone passwords.
- An action plan, which provides IT management with the steps required to bring systems into compliance with Alcatel-Lucent Enterprise best practices, and further guidance on how to strengthen security.
- A security checklist, which contains the complete list of items checked during the onsite audit. The current – and optimized - settings for each item are indicated, and guidelines for a technical expert (ACSE level) are provided to understand how and what to modify in the system.

## PRODUCT COVERAGE

The service is available for the Alcatel-Lucent Enterprise OpenTouch™ Suite for Mid-Sized and Large Enterprises (MLE) portfolio:

- Alcatel-Lucent Enterprise OmniPCX™ Enterprise Communication Server
- Alcatel-Lucent Enterprise OpenTouch Business Edition/Multimedia Services
- Alcatel-Lucent Enterprise Omnitouch™ 8400 Instant Communication Suite
- Alcatel-Lucent Enterprise OmniVista™ 4760/8770 Network Management System

## ASSISTANCE FOR RESTORING COMPLIANCE

This service only includes the stages detailed above: audit, action plan and security parameters checklist. If assistance is required to deploy the security recommendations and apply best practices to restore conformity, the Alcatel-Lucent Enterprise Professional Services experts can provide guidance throughout the process. Please contact the Alcatel-Lucent Professional Services at professional.services@alcatel-lucent.com for on-site assistance services such as:

- Impact assessment studies
- Change implementation
- Post-implementation configuration checks (control audits)

## INFORMATION AND REQUEST

For further information about the procedures associated with Alcatel-Lucent Enterprise Professional Services delivery and invoicing, please visit the Professional Services section on the Alcatel-Lucent Enterprise Business Portal, or send an email to professional.services@alcatel-lucent.com



Alcatel·Lucent Enterprise