

Secure IP Phones to Prevent Misuse and Toll Fraud

AND Phone is a powerful and scalable application platform for Unified Communications environments. The application server uses a modular base system which can be extended by services and functionalities you need for improving your communication tasks.

Securing your IP phone deployment reduces costs by eliminating toll fraud, protects the privacy of users by removing call entries on the IP phone and still allows you to be fully reachable.

Prevent IP phone misuse during off-business hours and protect the privacy of your employees. *AND Phone Lockout* ensures that only limited destinations are available when the phone is locked, like emergency services or the front desk, while incoming calls are still received.

Administration of the AND Phone server is completely centralized and uses a web-based frontend which can be extended by additional modules.

Benefits

- Prevent IP phone misuse
- Easy to operate for users
- Ensure confidentiality
- Locked phones still receive calls
- Works also with Extension Mobility
- Lockouts can be time-controlled
- Centralized PIN storage
- Full integration with other AND Phone applications

Features of AND Phone Lockout

AND Phone Lockout allows locking IP phones which limits the scope of numbers to call. Additionally the available Softkeys can be changed to limit the possible options on the IP phone and the directory entries for /received/placed calls are optionally deleted.

Even in the locked state the IP phone can receive incoming calls and reachability is fully available.



AND Phone Lockout offers multiple services to prevent misuse of IP phones and make sure that only defined numbers are allowed to be called.

Locking phones is simply done by starting a service - this can be placed even on a line button. Whenever a phone is locked the calling possibilities are limited to a defined calling search space but still the phone is fully reachable and incoming calls can be received.

Unlocking of phones is simply done by using the service again and specifying the username and password credentials.

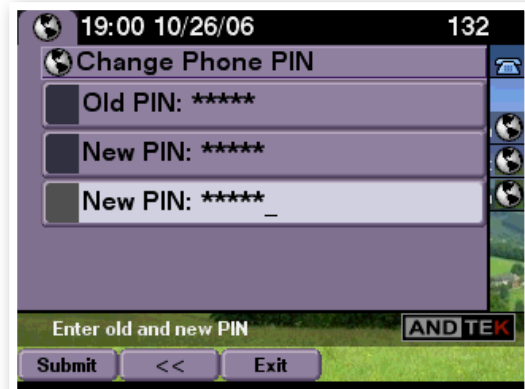


An automated service is available to lock phones at specific times. Therefore it is not possible that users are forgetting to lock their phone and misuse after working-hours is prevented.

Using the service requires usernames and PINs to authenticate the user. *AND Phone Lockout* offers multiple options using usernames of the existing environment. Besides managing the usernames directly on the *AND Phone Application Server* it is possible to use the Communications Manager database as well.

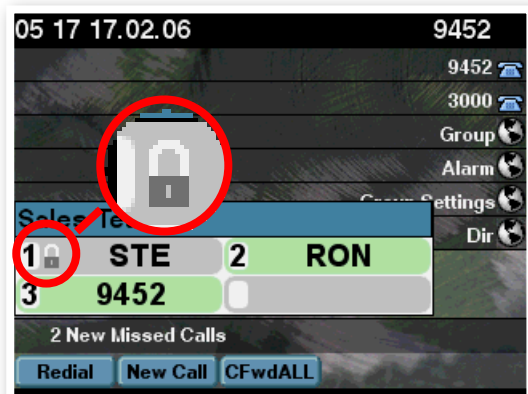
Using locally managed PINs or the Communications Manager database the PINs can be easily changed on the IP phone. Whenever PINs are changed they are automatically updated at the Communications Manager.

Another option is integration with LDAP directories where the user credentials are take out of the corporate directory, e.g. Active Directory.



Besides using *AND Phone Lockout* as standalone service it can be used in combination with the Communications Manager Extension Mobility service. In this case users can stay logged in but still lock their phone during lunch breaks or meetings.

When using the *AND Phone Group* service the status information about each user is automatically displayed on the IP phone which allows group members to see if a phone is locked. But the phone is still reachable and colleagues are able to set a callback.



That module can limited the access to additional *AND Phone* services like the connection to the corporate phone book if it is integrated with *AND Phone Directory*.

AND Phone Lockout

Services on the Phone

- Simple locking IP phone by a service
- Unlocking by using a PIN
- Locking with or without PIN
- Locked phones have limited reachability
- Locked phones are still reachable
- Time-based lockout for after-work hours
- Softkey templates changed for locked phones
- PINs can be changed directly on IP phone

Administrator Services

- Password protected access with multilevel administration
- Multi-level administration
- Centralized management of all *AND Phone* modules
- Users and PINs can be managed locally
- Users and PINs can be derived from Communications Manager
- External PINs can be retrieved from LDAP directory
- Integration to existing Communications Manager deployment
- Common usernames and PINs can be used
- Existing LDAP server can be used for authentication
- Integration with AND Phone Group
- Standalone deployment possible
- Works in conjunction with Extension Mobility
- Lockout of Extension Mobility users possible
- Common PIN available for both services
- Option to delete missed/received calls automatically
- Limited access to other AND Phone services if phone is locked

System Requirements

Server Requirements

- x86-based processor min. 2.8GHz
- Main memory 512MB/1GB/2GB
- Gigabit-/Fast-Ethernet interface
- Min. 20GB hard disc
- CD ROM drive
- Virtualization possible (VMware)

Software Requirements

- AND Phone Base
- AND Phone Lockout

Supported Operating Systems

- Linux (included)

Supported Telephone Systems *

- Cisco Unified Communications Manager 4.x, 5.x, 6.x, 7.x, 8.x

Supported Phones *

Cisco IP Phones 6900 series, 7900 series, 8900 series, 9900 series

* Available services might differ depending on the used type of phone and telephone system versions.



Am Soeldnermoos 17
85399 Hallbergmoos
Germany

T: +49 811 9594960
F: +49 811 95949676
E: info@andtek.com



Cisco®, Cisco IOS®, Cisco Systems® and the Cisco Logo are registered trademarks of Cisco Systems Inc.

ANDTEK®, AND Phone® and AND Mobile® are registered trademarks of ANDTEK GmbH.