SSP and Phone System Security

When you buy an Atos Unify telephone system you automatically receive 3 years of Unify Software Support, this means you will receive full system support along with software licence upgrades so your system stays current and protected at all times.

Continue your Success

After the 3 year period, your SSP needs to be renewed. This program is highly recommended and allows us to keep your system completely up to date and protected.

When choosing enterprise software, knowing your investment is protected is critical. You need to ensure you are always using the latest release of your software and that each release is secure. With SSP a combination of expert technical assistance, software updates, upgrades and access to comprehensive online resources are included.

For your peace of mind, you will know you have expert support standing by today, with upgrades for tomorrow.

Tips for a secure phone system

Like any device connected to the internet, VoIP phones can be targeted by hackers, many of these hackers are sophisticated and intend to hijack business phones for illicit calls leading to fraud, theft and other crime. Losing essential dollars to hackers can severely damage your bottom line. Secure settings, software updates and active monitoring of your phones router and phone system will help prevent intrusions, save you money, time and man power.

Protect credentials with strong passwords

Enable Network Address Translation (NAT)

Disable Phone web interface or have it managed

Close Port 80 with a Firewall

Disable International Calling

Protect credentials with strong passwords

Many VoIP systems with pre-set passwords left unchanged are easy targets due to pre-set passwords being available online your admin password should be the hardest to crack!

Enable Network Address Translation (NAT)

NAT is a feature on a router that provides your VoIP phones, computers and other devices with a private IP address that can only been seen on your local area network (LAN) . If a hacker cant discover your Private IP address then he cant manipulate and enter remotely.

NAT provides another layer of protection between your VoIP phone and any individuals who may try and exploit it.

Disable Phone web interface or have it managed

Your business phones web interface is probably its most vulnerable point of entry. it is a helpful tool when used in the right context, but can be a prime target for hackers who want t manipulate your business phone for fraudulent purposes

Close Port 80 with a Firewall

Port 80 is particularly susceptible to hackers because the traffic is HTTP, meaning hackers can potentially burrow into port 80 on your router and access the web interface as if it was a public website.

Until you close Port 80 your phones web interface will have a public IP address that anyone can access through the internet

Disable International Calling

If you don’t need to make international calls for your daily operations, it makes sense to completely disable international calling. If international calling is absolutely needed, make sure to regularly monitor your phone records

If you suspect you have been a victim of hacking, immediately disable the compromised device, generate a call detailed report to find out exactly joe many unauthorized calls were made using your phone system. Then call your service provider to report the incident and secure your devices.

About us

With a portfolio unequalled in its breath and flexibility, over 30 years’ experience and three national offices, Evotec are committed to designing, implementing and supporting innovative technology solutions based on the unique requirements of your business.

Contact Us

- 1300 133 996
- info@evotec.com.au
- service@evotec.com.au
- 02 9565 7233

Our offer

- National Customer Service access
- Certified Engineers and Field techs
- Post Sales Service
- Fully Managed Accounts