5 TIPS
for Wireless and BYOD

If your midsize company needs to deploy mobile devices, read on!

1 SITE SURVEY
Conduct a site survey before you deploy a wireless network.

Answer these key questions about your physical locations and the RF environment at each site:
- How many facilities will be included in the installation?
- What is the construction of the interior walls, cubicle walls, and external walls?
- Does the installation affect areas with sensitive equipment (such as labs), where you must limit or cannot install wireless?
- What types of wireless-enabled devices will be accessing the WLAN?
- Will your IT team perform a manual RF survey, or will you automate the process by using your WLAN's built-in site survey tools?

Read the Site Survey Guidelines for WLAN Deployment for more information.

2 DEPLOYMENT
Phase it in.

You can set up a wireless network with one functioning access point and expand from there.
- Site survey tools can help you deploy the rest of your access points, complete testing, and go live.
- Deploy your WLAN after work hours to minimize disruptions to your business during the workday.

3 SUPPORT
Be ready to support your employees and guests.

Providing support to your employees and guests is crucial to a successful deployment. Before your WLAN rollout, train your front-line technicians in how to troubleshoot your wireless network.
- Consider a phased deployment to avoid overloading your support staff.
- Think about providing a concierge service to senior management to smooth the on-boarding process.
- Have a clear escalation process in place to handle device connectivity issues.
- Put a guest access policy in place. Train lobby staff and employees on the steps for on-boarding guests. Keep it simple.

For more information about guest access deployment:
- Sign up for the Meraki Secure BYOD and Guest Access Webinar. Register now.
- Read the At-a-Glance: Cisco Unified Access: The Intelligent Platform for a Connected World

4 MANAGEMENT
Actively manage your wireless network and BYOD.

Don't just set it and forget it. Be proactive with your WLAN management.
- Look for usage patterns, irregularities, and RF interference.
- Maintain your device security policy to proactively manage secure user access and lost devices.
- Implement processes that allow administrators to quickly wipe business data and information from lost or stolen devices.

5 REPORTS
Assess, review, and take action.

Showcase the value of the WLAN to your leadership team. Use reports to validate how the WLAN is improving workforce productivity, engaging your customers, and delivering clear business results. Implement a plan that can report on:
- Number of users and devices connecting.
- Location and frequency of connections.
- Types of users and devices connecting: employees, partners, customers, and guests using company issued or bring-your-own-device (BYOD) laptops, tablets, smartphones, and RF-enabled devices, etc.
- Status of security mechanisms in place to protect users, data, and the network.
- Top five trouble-ticket issues.
- Compliance with regulatory rules such as Sarbanes-Oxley, Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry (PCI).

Case Studies

Safe and Reliable BYOD Collaboration:
Austrian radio station improves production quality with Cisco Identity Services Engine (ISE) and BYOD Smart Solution.
Read Now

Technology Innovation Fires Design Flair:
Cisco BYOD Smart Solution helps a furniture company enhance creativity and mobilize sales teams.
Learn More

CISCO

It's not what we make; it's what we make possible.
Learn how we can help you grow your business.

Visit our Midsize Website