Enabling Secure iOS® & iPadOS® in Closed Networks

Frequently Asked Questions

An introduction to the comprehensive solution, and the role of Owl's XD Tyton™, the secure gateway

For years, users in closed or otherwise air-gapped networks that wanted to use iPhone® and iPad® couldn't because there was no way to update them securely. A new, accredited architecture now makes it possible to use iOS® and iPadOS® inside classified and air-gapped environments. This FAQ introduces that solution to include how it's built, what each component of the comprehensive solution does, and where Owl Cyber Defense's XD Tyton™ fits in.

Challenge: The iOS & iPadOS Update Gap

Why couldn't iOS and iPadOS be leveraged securely in closed enclaves before?

To protect devices, a built-in capability on iPhone® and iPad® limits device communication to only approved endpoints, which is what makes secure use possible on air-gapped and other closed networks in the first place. However, that capability alone doesn't cover everything a device needs: it still must reach back out for update authorization, and until now there was no secure way to deliver that across a classified network boundary.

How is that update-authorization gap being solved?

A secure gateway, Owl's XD Tyton, closes it. It's the only approved way to deliver secure over-the-air software updates across a classified network boundary without a break in operational security. XD Tyton is one part of a larger, accredited architecture that enables secure iOS and iPadOS for air-gapped networks.

Closing the Gap with Owl's XD Tyton™

What does XD Tyton actually do, in simple terms?

Think of it as a secure translator at the boundary between your classified network and the outside world. When a device needs an update, XD Tyton carries the request out, retrieves the legitimate, authorized update, and brings it back in, fully inspectable by your existing security infrastructure, so nothing crosses the boundary unchecked.

Does XD Tyton replace our existing network security boundary?

No. That existing infrastructure is usually a Cross Domain Solution (CDS), and XD Tyton needs one in place to work at all, it's not a standalone product. XD Tyton handles one specific job on top of it: securely delivering software updates across the air gap.

A Comprehensive Solution to Secure Classified Mobility

How does XD Tyton fit into a comprehensive solution for secure classified mobility?

XD Tyton solves one critical piece, the update pathway, but a device still needs everything else in place to actually operate securely on a classified network: such as the device itself, device management, cloud infrastructure, and an accredited delivery partner. XD Tyton is one of five parts working together as a single architecture, not a standalone fix.

What does each component of the solution do?

The device itself provides the native foundation for secure closed-network use. Device management enrolls, configures, and enforces policy on every device. XD Tyton delivers the first and only secure update pathway for over-the-air (OTA) iOS and iPadOS updates across classified and air-gapped networks. Cloud infrastructure supports device management and app delivery at scale. And an accredited delivery partner brings the architecture together and sustains it over time.

Who is this solution for?

Organizations operating in defense, intelligence, homeland security, and law enforcement, along with allied and coalition partners, that need secure mobile access to classified or otherwise closed networks. If your team already uses iPhone or iPad in unclassified environments and wants that same experience extended into a classified one, this is for you.

What can our team do with this that they couldn't before?

Use a single iPhone or iPad, the device your team already knows, instead of juggling multiple hardened devices or locked-down alternatives. That includes secure communication, reading and annotating briefing documents, on-device AI for real-time translation, and building your own custom apps, all inside a classified environment.

How is this different from sticking with Android?

Classified mobility has largely relied on Android, often on customized builds needing separate, ongoing maintenance that lag behind the commercial version. This solution uses the stock, unmodified iOS and iPadOS your team already uses personally, so it receives the same security updates as consumer devices, on the same timeline, with no custom build or separate patch cycle.

Do we need all five components, or can we use what we already have?

No need to start from scratch. This is one adaptable architecture, not an all-or-nothing bundle. Many organizations may already have a component in place. Your starting point depends on what you have and what your mission requires.

Security & Compliance Considerations

Is this actually secure enough for classified use?

The architecture is purpose-built to meet rigorous government security requirements, not retrofitted later. It preserves the device's built-in hardware root of trust instead of weakening it, and every update crossing the boundary is inspectable and reviewable, with no black-box step a reviewer has to take on faith.

How does XD Tyton specifically comply with U.S. Government classified mobility requirements?

When integrated with an RTB-compliant HTN CDS, the combined architecture meets U.S. Government Raise the Bar and CSfC requirements for classified mobility.

Has the U.S. government approved or signed off on this?

Government accreditation bodies have been engaged throughout development, reviewing it on an ongoing basis. Formal accreditation for a given deployment follows your organization's own process. We're happy to walk your team through what that typically looks like.

Getting Started

How would we get started?

Your first step depends on what's already in place. An existing device management tool, cross-domain solution, or cloud environment can often join the starting architecture rather than be replaced. A short conversation with our team is usually the fastest way to map your environment to what you'd need.

Can we roll this out gradually?

Gradual rollout is common. Many organizations start with a pilot group, a specific mission need, or a single deployment option, and expand as it proves out, rather than committing to a full-scale rollout on day one.

Who do I contact to learn more?

Reach out to your Owl Cyber Defense representative or visit owlcyberdefense.com/product-xdtyton to connect with our team.