DATASHEET

Mission Ready Mobility
Zero Trust security for government agencies

Ivanti delivers access to classified networks on mobile devices – even in disconnected environments. That's a critical feature for a broad range of industries, notably including government agencies. The U.S. military has already selected Ivanti to deploy thousands of mobile endpoints to support the warfighter.

Ivanti for Tactical solutions align with the Commercial Solutions for Classified (CSfC) program for Mobile Device Management (MDM) and are designed to manage the full lifecycle of mobile endpoints in disconnected and/or tactical environments.

Compatibility

Our solutions are device-agnostic and offer integrations with rugged mobile device manufacturers including:

- Samsung
- Motorola
- Honeywell
- Zebra
- Getac

Additional compatibilities include:

- Integration with content management solutions.
- Integration with encrypted voice and text solutions.
- AppConfig implementation to customize ATAK.
- Integrated AppStore to manage and distribute ATAK iTAK app.
- Integrated PKI for certificate distribution.
- Integration with Privoro SafeCase for verifiable protections against remote surveillance via the mobile device's cameras and microphones and geofencing capabilities in secure workspaces.
- Integration with Redwall Technologies for multi-mode data separation and isolating secure personas on a single device.

Certifications and standards

Ivanti UEM makes it simple and seamless to manage diverse endpoints without compromising security. Ivanti is a leader in federal and DoD compliance and certifications. In addition to CSfC (NSA), security certifications and standards include:

- FIPS 140-2 Type I (FedRAMP MI GovCloud, Core, Sentry, Clients)
- SOC2 Type II (MI Cloud, Access)
- FedRAMP (MI GovCloud NA3)
- NIAP MDMPPv3 Common Criteria (Core 10, Agents – Feb 2019)
- NSA Commercial Solutions for Classified Program (Core 10, Agents – Feb 2019)
- DISA STIG (Core 10)
- CJIS
- EU-US Privacy Shield
- CSA STAR (Registered, Self-Assessment MI Cloud)

Lifecycle management

The general management lifecycle of a frontline worker device is comprised of 6 phases:

1. Provisioning.
2. Configuration.
3. Security and Control.
4. App deployment.
5. Monitoring and Compliance.
6. End of Life.

The provisioning of a device involves many steps including selecting a language, accepting the terms of agreement, connecting to your local Wi-Fi network and activating the device, among others. This complexity can result in a bottleneck, especially if multiple devices need to be provisioned for an enterprise.

Once the device has been provisioned, it is necessary for the device to be properly configured so it can be implemented into an environment for its intended use. In this case, the configuration phase begins with the download and installation of the DPC. This triggers a sequence of events including the installation of an MDM profile; the download of configurations, certificates and policies; and the enforcement of other configurations into the DPC itself.

Together with provisioning, proper configuration builds the security and control that an administrator requires to manage devices. With appropriate security and control in place, an administrator can enforce a complex pin or password, enforce updates to the device, or restrict the device to a single app or a kiosk mode.

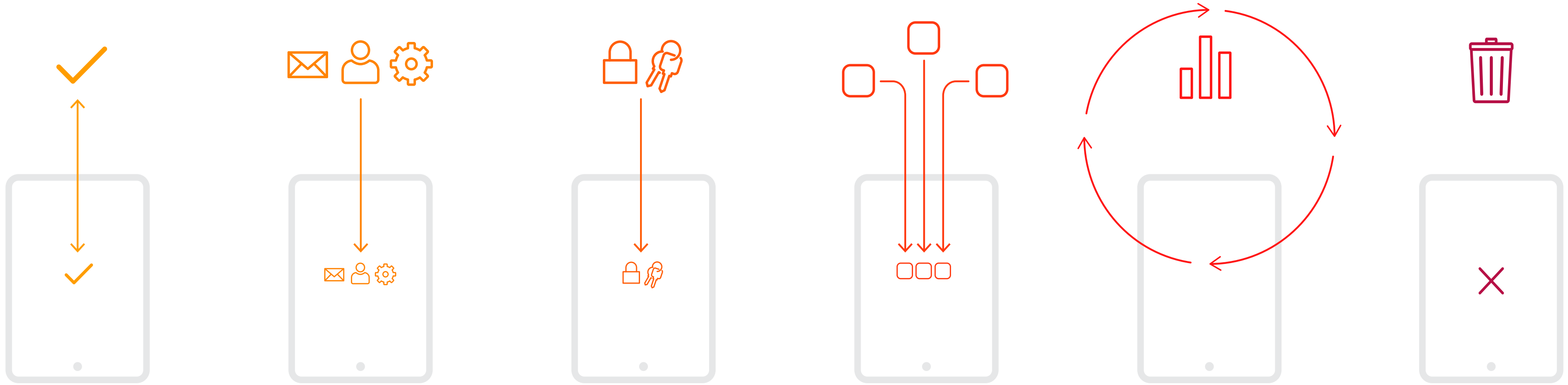
After the device has been provisioned, configured, and secured, the device is now ready for use. Ivanti supports apps from the Apple App Store, Google Play and Microsoft store, as well as custom in-house and private apps. Apps can be silently deployed or offered via the Enterprise App store. Apps are secured by means of AppConnect, Android Enterprise, O365 App Protection and Ivanti Tunnel.

When the end user has the tools required for their duties, the device and its enterprise data can be monitored for compliance issues, and if any arise, an administrator can act accordingly. These actions can vary from tiered compliance actions, to remote help using Help@Work, to wiping the device entirely.

Continuous validation of the device ensures a Zero Trust approach is applied to mobile devices connecting to enterprise networks. The solution ensures managed devices are secured in an automated and on-going compliant enforcement basis. Device, network, application, and phishing risks can be detected and automatically remediated on the device to protect enterprise data extended to mobile endpoints, if any of these risks are detected network access is denied automatically.

Finally, when the device is ready to be retired, an administrator has the choice of retiring or completely erasing the device.

Lifecycle management for frontline/remote worker devices



1

Provisioning

Prepare device for enrollment

Accept terms

Connect to Wi-Fi

2

Configuration

Download/install DPC

Certificates/ policies/ configurations

3

Security & control

Enforce policies compliant with DoD STIGs

MobileIron Threat Defense (MTD)

PIN/PW/requirement

Enforce updates/patches

4

App deployment

Enterprise app store

Silent install of apps

Remote configurations of apps (ATAK map servers)

Remote help

5

Monitoring & compliance

Ongoing/automated device compliance

Inventory management

Jailbreak/root detection

Threat defense & remediation

6

End of life

Retire

Wipe

Refresh

Ivanti for Tactical

Key benefits

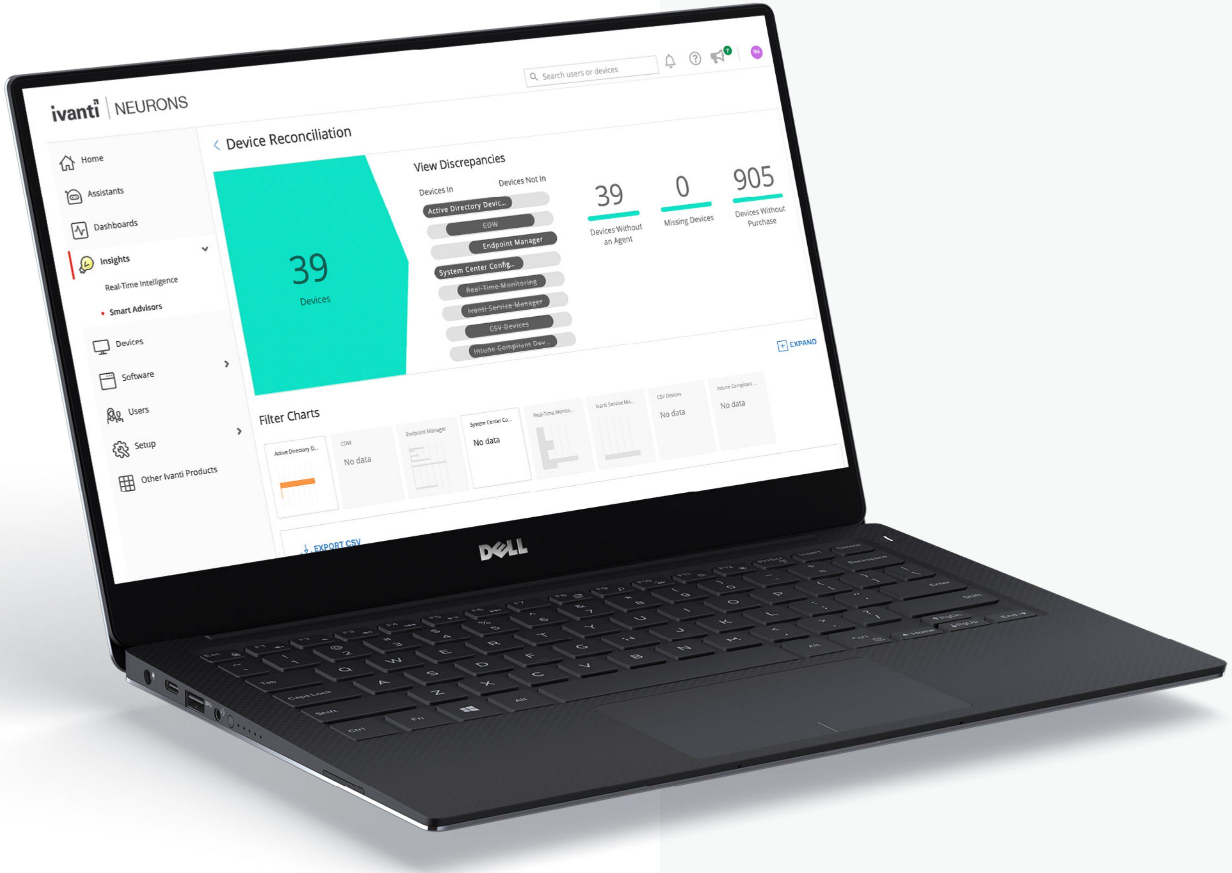
- Facilitates mission critical communications with edge computing technology.
- Fully functional with Android devices in an air-gapped secure network, and iOS devices with limited connectivity.
- Enables ATAK, iTAK, WinTAKVirtual Mobile Infrastructure (VMI) and other modern mobile apps.
- Tactical Assault Kit (TAK): map-based, Situational Awareness (SA) software apps across multiple platforms that provides tactical capabilities for military, federal government and Civil 1st Responder operations.
- Deploy, configure, and manage mission critical mobile applications such as encrypted voice and text on disconnected networks.

Security and power when it counts

Ivanti for Tactical is uniquely capable of delivering a top-tier UEM that isn't limited by a disconnected environment. The ability to deploy a highly certified virtual appliance and a solution that's device-agnostic with full lifecycle management means secure, user-friendly and continuous access in high-stakes applications.

About Ivanti

Ivanti makes the everywhere workplace possible. In the everywhere workplace, employees use myriad devices to access IT applications and data over various networks to stay productive as they work from anywhere. The Ivanti Neurons automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a unified IT platform that enables devices to self-heal and self-secure and empowers users to self-service. Over 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure, and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com



ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com