A clear path to FedRAMP High: Migrate with confidence

Imagine a government agency where employees work securely from anywhere, thanks to modern UEM capabilities. Robust security measures streamline compliance and reduce vulnerabilities through centralized policies and automated audits, simplifying the entire device lifecycle.

By migrating to Workspace ONE UEM FedRAMP-authorized SaaS, your agency can achieve this level of security and efficiency, transforming device management by strengthening compliance, boosting performance, and reducing operational overhead. This move accelerates your journey to a modern, highly reliable device management platform, enabling your agency to focus on mission-critical tasks with confidence.

How Omnissa helps the government migrate

- Expert planning and assessment of current on-premises configurations.
- Setup of parallel cloud environments and directory integrations.
- Doesn't require device re-enrollment.
- Change management strategies help minimize user disruptions while maintaining security policy updates.
- Support for configuring authentication methods, access policies, and Hub Services.
- Assistance with application migration, testing, and post-migration optimization.

omnissa®

Compliance without complexity

FedRAMP High GovCloud services

- Workspace ONE UEM, Omnissa Access, Intelligent Hub, and Omnissa Intelligence are already authorized at FedRAMP High and hosted in AWS GovCloud, so agencies can “migrate into” an existing compliant environment instead of building everything themselves.
- This lets programs inherit a large set of NIST 800-53 controls (encryption, hardening, monitoring, vulnerability management) from Omnissa SSP and continuous monitoring package during migration.

Migration paths from existing Omnissa/on-prem

- Omnissa documents migrations from on-premises components (for example, Omnissa Access on-prem and ENS servers) into cloud tenants, including the FedRAMP domain, using federation and staged cutover rather than big-bang replacement.
- These guides cover standing up the new tenant, establishing SAML trust, moving directories and virtual app collections, and then re-pointing users —patterns that apply directly when the target tenant is the FedRAMP GovCloud environment.

Security controls that simplify ATO and re-authorization

- The FedRAMP environment includes FIPS-validated crypto, DoD STIG/CIS Level 2 hardening, tight privileged access controls (U.S.-person only, hardware token MFA), automated vuln management with FedRAMP timelines, and 24×7 FedRAMP-specific SOC.
- Because those controls are already assessed and continuously monitored, agencies can reference Omnissa FedRAMP High package, monthly ConMon reporting, and customer-facing POA&M/CRM artifacts when updating their own ATO after migration.

Support for DOD / CMMC and hybrid federal use

- The FedRAMP High environment hosts a DOD only Workspace ONE instance that is in process for a DoD CC SRG IL4 provisional authorization.
- Omnissa hosts a CMMC Level 2 certified repo within the FedRAMP boundary to handle CUI.
- Customers can confidently utilize Workspace ONE to meet their own CMMC use cases. The FedRAMP authorization is augmented select artifacts modified in a NIST 800-171 aligned format.
- GovRAMP and TxRAMP reciprocity means that SLED customers can confidently migrate to the FedRAMP High system while relying on the managed compliance services provided by the GovRAMP program to reduce costs and compliance overhead.

Practical migration assistance

Omnissa provides tenant provisioning in the FedRAMP domain and includes customers in monthly continuous-monitoring sessions, giving them ongoing guidance as they move workloads and devices. Knowledge base updates and best-practices notes around UEM SaaS migrations and IP changes further support phased moves and minimize disruption during the migration process.

FedRAMP Migration Checklist

Assess the current environment

Inventory directories (AD/LDAP), connectors, authentication methods (e.g., certificates, Mobile SSO), access policies, Hub Services, web apps, virtual app integrations (Horizon), OAuth clients, and branding. Document which apps and user groups are in scope first so you can migrate in phases instead of all at once.

Provision the FedRAMP cloud tenant

Work with Omnissa/account teams to provision a Workspace ONE tenant in the FedRAMP GovCloud environment rather than a commercial region. Perform initial setup: tenant URL, admin access, and basic configuration so it can run in parallel with your existing instance.

Rebuild core integrations in FedRAMP

Install and configure the new Omnissa Access/Workspace ONE UEM connectors so the FedRAMP tenant can talk to your on-premises AD/LDAP and identity systems. Recreate authentication methods and access policies in the FedRAMP tenant, taking advantage of any cloud-only methods you plan to use in the future.

Establish trust between old and new

Set up SAML federation between the existing Workspace ONE environment and the new FedRAMP tenant so users can authenticate once and reach resources during transition. Configure the old tenant as an application source in the new tenant and verify that test users can log in to the FedRAMP tenant and launch applications successfully.

Migrate users and UEM settings

Start by syncing a pilot group of users into the FedRAMP tenant, validate their experience, and then bring over remaining users in waves. Migrate UEM-related settings (profiles, compliance policies, device settings) so managed devices can be evaluated and enforced by the FedRAMP tenant without breaking access.

Migrate web apps and virtual desktops

For each web app, update federation so the app trusts the FedRAMP tenant as its IdP; use export/import tools where available to speed web-app configuration. Recreate and point Horizon virtual app collections at the FedRAMP tenant and update connection server configurations accordingly.

Test thoroughly, then decommission legacy. Conduct end-to-end validation of authentication, application access, device compliance, and administrative workflows, remediating any issues prior to full cutover. Once all users and use cases are operating in the FedRAMP environment, update DNS and URLs to point to the FedRAMP tenant and decommission the legacy environment.

Agencies streamline authorization efforts by aligning their documentation and ATO packages with the FedRAMP High Workspace ONE environment, allowing them to inherit Omnissa-assessed controls rather than re-implementing them independently.

Ready to migrate?

Make sure you visit omnissa.com/platform/federal and stop by the Omnissa trust center for more details. When you're ready, **connect with your Omnissa Federal Government sales representative** to discover how to transform secure collaboration.

omnissa®