datto
A Kaseya COMPANY

FIPS Mode for Datto SIRIS

Secure backup and recovery for regulated environments

FIPS Mode empowers managed service providers (MSPs) and internal IT teams to deliver government-grade data protection for organizations operating in regulated sectors, including federal, state and local government, education, financial services and health care.

Available at no additional cost, this optional mode introduces FIPS 140-3 validated encryption across Datto SIRIS 6 appliances, including Datto Windows and Linux agents. By enabling FIPS Mode, MSPs and IT teams can meet strict compliance mandates without sacrificing the performance, simplicity or seamless continuity Datto is known for.

With FIPS Mode, Datto becomes the first cyber resilience platform to deliver FIPS-validated cryptography across the entire backup-to-cloud stack, setting a new standard for secure, compliant data protection and business continuity.

FIPS 140-3™

Secure by design

Simplicity and security work hand in hand. FIPS Mode is activated seamlessly on any SIRIS 6 appliance, including rackmount, mini PC and desktop form factors.

- **Built for compliance-driven environments:** Deliver protection that meets government, defense and regulatory standards.
- **Streamlined management:** Control everything from a single, secure cloud portal with full visibility into protected systems.
- **Fast deployment:** Get compliant backups up and running in minutes by activating FIPS Mode on your turnkey Datto SIRIS 6 appliance.

Scale cyber resilience confidently, knowing all backup operations use FIPS 140-3 validated encryption algorithms.

Compliance beyond backup

FIPS Mode doesn't just secure data at rest — it fortifies the entire data protection lifecycle.

- **Backup:** Inverse Chain Technology™ ensures every incremental backup is a fully independent recovery point, protected with FIPS 140-3 validated encryption for both Datto Windows and Linux agents.
- **Virtualization:** Local virtualization, including Rescue Agent for crash-consistent virtual machine (VM) backups and cloud virtualization for rapid recovery.
- **Restore:** File restore, image export, ESX upload, cloud file/folder recovery and bare metal restore (BMR).
- **1-Click Disaster Recovery:** Build and test recovery configurations in the Datto Cloud at no additional cost, then replay and activate DR with a single click.

With Datto's Recovery Launchpad, you can perform rapid restores and spin up systems in the Datto Cloud directly from the secure web portal, minimizing downtime and ensuring alignment with your recovery objectives.

The Datto Cloud advantage

Not all clouds are created equal. The immutable Datto Cloud is purpose-built for secure backup, replication and recovery with FIPS 140-2 Inside today and FIPS 140-3 Inside planned for early 2026.

- **Immutable architecture** prevents tampering or deletion.
- **Geographically distributed data centers** ensure resilience and redundancy, providing a robust infrastructure.
- **1-Click Disaster Recovery** launches virtual environments instantly.
- **Flat-fee Disaster Recovery-as-a-Service (DRaaS) model** means no hidden compute or testing costs.

Datto's cloud infrastructure provides the same reliability and scalability MSPs and IT teams expect, now reinforced with FIPS-validated cryptography for compliance-aligned workloads.

Security and confidence in a ransomware world

FIPS Mode enhances Datto's already robust security stack with cryptographic controls validated by the National Institute of Standards and Technology (NIST), ensuring data is safeguarded from emerging cyberthreats.

- Two-factor authentication for portal access
- Hardened backup appliances and agents
- Immutable cloud storage with Cloud Deletion Defense™
- Encrypted replication between sites and the cloud

Every layer of Datto's FIPS Mode, from local backups to cloud restores, is designed to maintain compliance integrity while defending against sophisticated attacks.

FIPS components overview

Component	Cryptography level	Description
SIRIS 6 appliances	FIPS 140-3 Inside*	End-to-end protection for local backup, recovery and virtualization.
Datto Windows agent	FIPS 140-3 Inside*	Collects and transmits encrypted data using FIPS-validated cryptography.
Datto Linux agent	FIPS 140-3 Inside*	Collects and transmits encrypted data using FIPS-validated cryptography.
Datto Cloud	FIPS 140-2 Inside*	Current validation at OS level; FIPS 140-3 Inside planned for 2026.

*See the Appendix: Technical references for a full list of certificates.

Unbreakable cyber resilience

FIPS Mode is created for cyber resilience, combining the reliable, turnkey Datto SIRIS platform with the assurance of FIPS-validated encryption.

- **Unified continuity:**
  Protect Windows and Linux workloads with a fully integrated hardware, software and cloud solution.
- **Seamless management:**
  Control everything through the Datto Partner Portal — a single pane of glass for all protected workloads.
- **Training and support:**
  Leverage Datto's "24 by forever" technical support and on-demand training for seamless adoption.

Delivering secure continuity has never been simpler. With Datto FIPS Mode, MSPs and IT teams can confidently serve organizations in regulated industries while maintaining the same reliability, automation and recovery performance that define Datto.

Appendix: Technical references

FIPS Mode utilizes the following validated modules:

Datto SIRIS 6, Datto Windows agent, Datto Linux agent

- FIPS 140-3 Inside Certificate #5040
- FIPS 140-3 Inside Certificate #4794
- FIPS 140-3 Inside Certificate #4894

Datto Cloud

- FIPS 140-2 Inside Certificate #4292
- FIPS 140-2 Inside Certificate #4366
- FIPS 140-2 Inside Certificate #3902
- FIPS 140-2 Inside Certificate #4046

These components ensure FIPS-validated controls at the OS and cryptographic library level, verified through NIST's Cryptographic Module Validation Program (CMVP).