Release Notes for Cisco Hypershield, Release v10.0.0.0

2026-08-21

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Hypershield

Cisco Hypershield 10.0.0.0 is the initial generally available release of the Cisco Hypershield offering.

This Hypershield release applies to the following components:

- Hypershield Controller v10.0.0.0
- Hypershield Agent Gateway (AGW) v10.0.0.0
- Hypershield Network Enforcer (FWA) v10.0.0.0
- Hypershield Deployment Appliance v10.0.0.0
- Cisco Cloud Control (August 2026 or newer)

New software features

This section provides a brief description of the new software features introduced in this release.

Table 1. New software features for Cisco Hypershield, Release 10.0.0.0

Component affected	Feature name	Description
Hypershield Controller	Management User interface: Timescape	Provides browser-based management of policies, objects, deployments, events, and system status.
Cisco Cloud Control	Management User interface: Cisco Cloud Control	Integration and access to the Management User Interface through Cisco's cloud-based management platform as an option.
Hypershield Controller	Programmatic Access: RestAPI	Automates supported network-object and security-policy operations through versioned REST endpoints.
Hypershield Controller	Leader Controller	On-premise virtual appliance hosts management services and maintains the authoritative policy configuration and propagates it down to all followers.
Hypershield Controller	Follower Controller	An on-premise virtual appliance that hosts the control plane services and distributes approved policy to connected enforcement points and reports deployment status. Multiple Follower Controllers may be deployed inside or across multiple data centers connected to the same Leader Controller.
Hypershield Controller	Backup/Restore	Protects and restores the controller state, configuration, policy data, and authorization to meet recovery requirements.
Hypershield Controller	Authorization/RBAC	Integration with existing OIDC Providers for authorization and control of administrative access through assigned roles and permissions.
Hypershield Controller	Policy Management	Supports creating, reviewing, deploying, and monitoring security policies based on Network Object Groups using Labels and/or VLAN/VRF/CIDR and Port and Protocol constructs.
Hypershield Controller	Network Object Groups	Organizes reusable network objects into small groups that are then labeled or directly leveraged for policy management.

© 2026 Cisco and/or its affiliates. All rights reserved.

Hypershield Controller	Telemetry	Centralized configuration of logging groups and destinations for operational and flow data via Syslog and IPFIX.
Hypershield Deployment Appliance	Hypershield Controller Deployment Automation	A management VM (virtual machine) that automates controller deployment and initial leader and follower cluster configuration leveraging the hypervisor management API.

New hardware features

This section provides a brief description of the new hardware features introduced in this release.

Table 2. New hardware features for Cisco Hypershield, Release 10.0.0.0

Product impact	Feature	Description
Hypershield Agent Gateway (AGW)	Automated Policy Placement	Delivers approved policies to the appropriate Hypershield Network Enforcer inside the Smart Switch just in time based on the NX-OS Switch Configuration.
Hypershield Agent Gateway (AGW)	Logging Export to Multiple Destination	Streams audit and enforcement events to multiple configured syslog destinations directly from the Hypershield Agent Gateway running in each Smart Switch.
Hypershield Network Enforcer (FWA)	IPFIX Telemetry Export to Multiple Locations	Streams IPFIX flow records to multiple configured collectors destinations directly from the Hypershield Network Enforcers running in each Smart Switch.
Hypershield Network Enforcer (FWA)	Stateful L3/L4 Policy Enforcement	Enforces Layer 3 and Layer 4 policy on unicast network flows steered to the Network Enforcer in each Smart Switch.
Hypershield Network Enforcer (FWA)	Active/Active State Synchronization	Synchronizes connection state between paired Smart Switches for resilient traffic processing.

Caveats and limitations

This table lists the limitations for this release. Information related to current limitations of the platform. Best practices are provided to help guide the Operator.

Table 3. Known issues for Cisco Hypershield, Release 10.0.0.0

Description	Component	Impact	Workaround
Policy and network object payload size	Hypershield Controller	A SmartSwitchNetworkPolicy or NetworkObjectGroup serialized above 1.5 MB can fail when the follower Kubernetes API materializes it.	Keep each object below 1.5 MB. Split large policies or object groups into smaller reusable objects.

© 2026 Cisco and/or its affiliates. All rights reserved.

OIDC refresh-token flow	Hypershield Controller	Users must authenticate again when the ID token expires, even when the identity provider supplies offline access.	Plan for periodic re-authentication and choose an appropriate ID-token lifetime in the identity provider.
Event-history CSV export	Hypershield Controller	A CSV export contains only the events displayed on the current page, not the complete filtered result set.	Export each page and combine the files, or review the complete history in Timescape.
Leader enrollment event visibility	Hypershield Controller	Leader enrollment events are not shown in event history, so enrollment does not create a visible audit entry in the UI.	Record leader enrollment through the organization change-control process.
Telemetry configuration replacement	Hypershield Controller / Hypershield Agent Gateway	A pre-existing statically named syslog or IPFIX ConfigMap can prevent a new UI-managed configuration from reaching previously configured Smart Switches.	Remove the obsolete ConfigMap from the affected follower cluster, then reapply the telemetry configuration and verify delivery.
VM live migration	Hypershield Network Enforcer	Live migration of a protected workload VM resets established TCP sessions that traverse DPU stateful inspection.	Drain connections or schedule migration during a low-traffic maintenance window.
Policy updates during control-plane disconnection	Hypershield Agent Gateway	A disconnected Smart Switch continues enforcing its last installed policy in a fail-closed posture, but it cannot receive new policy.	Restore follower-to-switch connectivity before deploying policy changes.
Policy restore after Smart Switch power cycle	Hypershield Network Enforcer / Agent Gateway	A power cycle clears in-memory DPU policy. Traffic is fail-closed until the switch reconnects and the control plane restores the current policy.	Use a correctly configured HA partner to maintain enforcement while the rebooted switch recovers.
Broadcast, unknown-unicast, and multicast traffic	Hypershield Network Enforcer	BUM traffic bypasses the DPU and is not evaluated by Hypershield policy.	Use NX-OS controls such as storm control or IGMP snooping; do not rely on

© 2026 Cisco and/or its affiliates. All rights reserved.

			Hypershield policy for BUM filtering.
Bidirectional policy on L2-only switches	Hypershield Network Enforcer	On a switch without routed interfaces, policy can be unidirectional if both source and destination VLANs are not steered to the DPU.	Configure both VLAN IDs in the service firewall block and validate traffic in both directions.
Inter-VRF mode counters	Hypershield Network Enforcer	Inter-VRF mode is enabled by default. The first packet makes two NPU-to-DPU passes, which can double-count dropped packets on the service Ethernet interface.	Account for the double count in monitoring. Disable inter-VRF mode only for an intra-VRF-only design and only through an approved procedure.
Very large policy deployment	Hypershield Network Enforcer / Agent Gateway	Applying more than 500,000 rules can temporarily reduce throughput while the receiving Smart Switch programs the policy.	Schedule very large deployments during lower traffic and monitor switch health and policy status until synchronization completes.
Policy references a missing VRF	Hypershield Controller	The policy remains Pending and rules that depend on the missing VRF are not enforced on that Smart Switch.	Configure the referenced VRF. If its absence is intentional, treat Pending as expected for that target.
Policy references a missing VLAN	Hypershield Controller	The policy remains Pending and rules that depend on the missing VLAN are not enforced on that Smart Switch.	Configure the referenced VLAN. If its absence is intentional, treat Pending as expected for that target.
Mixed IPv4/IPv6 endpoint rule	Hypershield Controller	A policy that pairs principal and resource from different IP families remains Pending and is not enforced.	Use IPv4-to-IPv4 or IPv6-to-IPv6 source and destination pairs.
Policies reference mismatched VLAN IDs in Network Object Groups	Hypershield Controller	Policies using VLAN-based objects are only enforced when principal and resource VLANs match. Use VRF-based objects for inter-VLAN	For inter-VLAN enforcement policies, create policies using network object groups that leverage VRF, not VLAN, IDs.

© 2026 Cisco and/or its affiliates. All rights reserved.

		traffic.	

Open issues

This table lists the open issues in this release.

Table 4. Open issues for Cisco Hypershield, Release 10.0.0.0

Description	Component	Impact	Workaround
Policy Deployment status shows in-sync when the deployment is still pending	Hypershield Controller	After a policy is edited or redeployed, the deployment status may continue to show “In Sync” instead of “Pending” until the updated version reaches the network switches. This window is more pronounced if hubble-timescape-intent-syncer is temporarily unavailable.	Wait for policy update to refresh.
Smart Switch HA failover	Hypershield Network Enforcer	Failover can take up to 10 seconds, and some connections can be interrupted during convergence.	Design applications to retry transient failures and validate the HA peer path before production use.

© 2026 Cisco and/or its affiliates. All rights reserved.

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved.