Current Technologies
Computer Learning Centers

☎ +1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

CISCO Partner
Platinum Learning

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Cisco SD-WAN UX 2.0 Topology, Configuration Groups and Policy Groups Migration

Cisco SD-WAN UX 2.0 Topology, Configuration Groups and Policy Groups Migration

This Cisco SD-WAN UX 2.0 Topology, Configuration Groups and Policy Groups Migration official Cisco course is critical for companies running Cisco SD-WAN because Cisco is fundamentally changing how SD-WAN environments are designed, deployed, and operated. The transition from device templates, feature templates, and traditional centralized policies to configuration groups, policy groups, and topology-based workflows represents more than a UI refresh; it is a shift in the operational model of Cisco SD-WAN Manager. Organizations that continue to rely on legacy UX 1.0 concepts without understanding UX 2.0 risk misconfigurations, slower deployments, and operational blind spots as Cisco continues to enhance and prioritize the new interface. This training equips teams with a clear understanding of how configuration groups replace complex template hierarchies, how policy groups simplify policy lifecycle management, and how topology-aware workflows improve visibility and intent-based design across the WAN, all of which are essential to maintaining operational efficiency and consistency in modern SD-WAN deployments.

Equally important, this class prepares organizations for real-world migration and coexistence scenarios that are already common in production networks. Many enterprises are operating mixed environments where some devices remain on UX 1.0 while others adopt UX 2.0, creating operational complexity if teams lack the proper skills and migration strategy. The course provides structured guidance on pre-migration checks, validation, rollback planning, and troubleshooting in the new interface, ensuring that teams can transition safely without disrupting business-critical connectivity. As Cisco continues to innovate around topology visualization, policy correlation, and automation within UX 2.0, companies that invest in this training position themselves to adopt new features faster, reduce operational risk, and maintain long-term supportability of their Cisco SD-WAN environments

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Course Duration

4 days

Course Price

$3,795.00 or 38 CLCs

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Who Should Attend

The primary audience for this course is as follows:

- Network Engineers who configure, optimize, and troubleshoot Cisco SD-WAN environments.
- SD-WAN Administrators responsible for managing device configurations, policies, and network monitoring through Cisco vManage.
- Solution Architects designing SD-WAN deployments and planning UX 1.0 to UX 2.0 migration strategies.
- Operations and NOC Teams requiring real-time monitoring, topology analysis, and policy verification in UX 2.0.
- IT Managers overseeing SD-WAN operations, ensuring standardization, and aligning deployments with business objectives.

- Consultants and Cisco Partners assisting customers in migrating from UX 1.0 to UX 2.0 and managing mixed environments.

Prerequisites

- Installing, Configuring, Monitoring, and Troubleshooting Cisco Catalyst SD-WAN
- Implementing Cisco SD-WAN Solutions (ENSDWI)
- Cisco SD-WAN Equivalent Knowledge

Module 1: Catalyst SD-WAN Platform Overview

- Lesson 1: SD-WAN WAN Architecture Overview
    - Review SD-WAN architecture fundamentals.
- Lesson 2: Cisco SD-WAN Solution Overview
    - Overview of Cisco SD-WAN platform.
- Lesson 3: Licensing for Cisco SD-WAN
- New Features by Version

Module 2: Understanding the Evolution: UX 1.0 vs UX 2.0

- Interface and Navigation Changes
    - Modernized dashboard with customizable widgets and improved performance.
    - Unified configuration and policy management under Configuration Groups and Policy Groups.
    - Simplified navigation with fewer clicks to reach common tasks.
- Workflow Enhancements
    - Separation of "Modify" and "Deploy" stages for better change control.
    - Real-time validation and pre-deployment checks to reduce errors.
    - Improved topology view with integrated policy visualization.
- Feature Advancements
    - Introduction of Feature Profiles and Feature Parcels for modular configuration.
    - Policy Groups consolidating application, security, and topology policies into a single interface.
    - Advanced search, filtering, and bulk actions for faster operations.
- Operational Improvements
    - Faster page load times and responsive interface for large-scale deployments.
    - Centralized catalog integration for importing Cisco-provided configurations and policies.
    - Enhanced troubleshooting capabilities with time-based topology replay and contextual action menus.
- Key Differences Summary Table
    - Side-by-side comparison of UX 1.0 vs UX 2.0 in terms of configuration, policy, monitoring, and troubleshooting.

Lab 1: Side-by-Side Comparison

- Open both UX 1.0 and UX 2.0 environments.
- Perform identical tasks (e.g., check device status, locate templates, view alarms) in both versions.
- Document time differences and navigation improvements.

Module 3: Navigating the UX 2.0 Interface

- Dashboard Overview and Changes
    - Modernized landing page with customizable widgets for device health, alarms, application performance, and active policies.
    - Quick-access panels for recent tasks, alerts, and deployment history.
- Primary Navigation Menu
    - Consolidated menu with sections for Monitor, Configuration, Policy, and Administration.
    - Context-sensitive menus that adjust options based on the selected view.
- Configuration Section

  - Introduction to Configuration Groups, Feature Profiles, and Parcels.
  - Device inventory view with tagging, filtering, and bulk action support.
- Policy Section
  - Access to Policy Groups, including Application Priority, Security, and Topology.
  - Policy object management for reusable configuration components.
- Monitoring and Topology
  - Real-time and historical topology views with health overlays.
  - Policy visualization showing live traffic paths and policy application points.
  - Integrated alarms, logs, and event correlation.
- Search and Filtering Tools
  - Global search bar for devices, policies, and configuration elements.
  - Advanced filters by site, device type, VPN, or status.
- User Experience Enhancements
  - Reduced click depth for common tasks compared to UX 1.0.
  - Faster page load times and responsiveness for large deployments.
  - Drag-and-drop support in certain configuration workflows.
- Best Practices
  - Customize the dashboard with widgets relevant to your operational priorities.
  - Use tagging and filters to quickly isolate devices during troubleshooting.
  - Regularly review active alarms from the dashboard to spot early issues.
  - Leverage the Modify vs. Deploy workflow for safe, staged changes.

Lab 2: UX 2.0 Interface

- Log in to UX 2.0, explore the dashboard, and customize widgets.
- Navigate to Configuration Groups, locate a device, and view its associated profiles.
- Access Policy Groups, filter for a specific VPN, and examine an application priority policy.
- Use the topology view to locate a device, apply a performance overlay, and view active policies.

Module 4: Templates and Configuration Groups Optimization in UX 2.0

- Introduction to Configuration Groups
  - Replaces UX 1.0 monolithic device templates with a modular, reusable configuration model.
  - Organizes device settings into logical Feature Profiles and Feature Parcels for granular control.
  - Enables faster configuration updates by reusing parcels across multiple groups.
- Configuration Group Structure
  - Configuration Group: Top-level container that defines the overall device configuration.
  - Feature Profile: Logical grouping of related settings (e.g., System, VPN, Security, Routing).
  - Feature Parcel: The smallest reusable configuration block (e.g., a specific VPN interface or QoS policy).
- Creating Configuration Groups
  - Select devices or tags for assignment.
  - Add Feature Profiles relevant to the device role.
  - Populate Feature Parcels with required settings.
- Modifying and Deploying Changes
  - Modify Stage: Make changes without impacting live devices.
  - Deploy Stage: Push changes to devices after validation.
  - Deployment previews to show exactly what will be applied.
- Versioning and Reuse
  - Track revisions of Configuration Groups for change control.
  - Reuse Feature Parcels across multiple groups to maintain configuration consistency.
- Integration with Policy Groups
  - Configuration Groups define device-level settings.
  - Policy Groups define application, security, and topology rules.

    - Both work together to provide full device behavior control.
- Best Practices
    - Use tags to group devices logically (by role, region, or function) for easier Configuration Group assignments.
    - Keep Feature Parcels small and focused to increase reusability.
    - Document changes in Configuration Group descriptions for audit purposes.
    - Always validate changes in the Modify stage before deploying to production.

Lab 3: Creating Configuration Groups

- Create a new Configuration Group for a branch router and assign Feature Profiles for System and VPN.
- Add and modify Feature Parcels for routing and QoS.
- Use the Modify stage to preview configuration changes before deployment.
- Deploy the Configuration Group to a test device and verify the applied configuration.

Module 5: Policy Groups in UX 2.0

- Introduction to Policy Groups
    - Differences from UX 1.0 policy workflows
    - Unified interface for all policy types
    - Intent-based design and faster deployment
- Policy Group Components
    - Application Priority Policies: Define traffic handling based on application performance requirements using SLA classes, preferred paths, and failover criteria.
    - Security Policies: Integrate ZBFW, IDS/IPS, URL filtering, AMP, and DNS security directly into the policy workflow.
    - Topology Policies: Define traffic flow patterns such as hub-and-spoke or mesh; only one topology configuration can be active at a time in UX 2.0.
    - Groups of Interest (Policy Objects): Application lists, prefix lists, community lists, and other reusable objects that form the building blocks of policies.
- Workflow Improvements in UX 2.0
    - Single creation point for all policies.
    - Ability to create simple or advanced layouts depending on the use case.
    - Preview of CLI-equivalent configuration before deployment.
- Policy Catalog Integration
    - Importing Cisco-provided policy profiles for rapid deployment.
    - Customizing catalog policies to match organizational requirements.
- Deployment Process
    - Associating Policy Groups with devices or sites.
    - Applying device/site-specific variables.
    - Monitoring enforcement via the UX 2.0 topology view and policy dashboards.
- Best Practices
    - Keep application priority definitions aligned with business-critical service levels.
    - Standardize security policy profiles to enforce uniform protection across all sites.
    - Validate topology changes in a lab or test region before production rollout.
    - Use policy objects for scalability and easier updates.

Lab 4: Building and Applying Policy Groups

- Create a Policy Group for VoIP prioritization using Application Priority.
- Add a security profile with URL filtering and IPS for guest network VPNs.
- Configure a hub-and-spoke topology within the Policy Group.
- Deploy the Policy Group to multiple sites and verify impact using UX 2.0’s topology and performance views.

Module 6: Topology in UX 2.0

- Topology Overview in UX 2.0
  - Topology definition through Topology Policy Groups.
  - Relationship between topology, application-aware routing, and VPN segmentation.
  - Visualization enhancements in UX 2.0 for policy-aware topology views.
- Full Mesh Topology
  - Overview: Direct site-to-site connectivity between all participating sites.
  - Use cases: Low-latency inter-branch communication, distributed workloads.
  - Configuration in UX 2.0:
    - Create a new Topology Policy Group.
    - Select VPN(s) for inclusion.
    - Choose Full Mesh topology type and assign sites or site lists.
    - Deploy and validate using the topology map.
- Hub-and-Spoke Topology
  - Overview: Centralized connectivity where all spokes communicate via one or more hub sites.
  - Use cases: Centralized security services, branch-to-data-center connectivity.
  - Configuration in UX 2.0:
    - Create a Topology Policy Group.
    - Define hub sites and spoke sites.
    - Assign VPN(s) and apply to device/site lists.
    - Deploy and validate that spoke-to-spoke traffic routes via the hub.
- Custom Topology
  - Overview: Tailored connectivity patterns for hybrid or specialized environments.
  - Use cases: Regional hubs, selective site interconnection, test environments.
  - Configuration in UX 2.0:
    - Create a Topology Policy Group.
    - Use Custom topology type.
    - Define specific site-to-site links and routing behavior.
    - Deploy and confirm through policy visualization.
- Topology Validation
  - Use real-time topology view to confirm policy enforcement.
  - Apply overlays to show link quality, application flows, or policy paths.
  - Use historical playback to confirm stability over time.
- Best Practices
  - Always test new topology policies in a lab or limited pilot before network-wide deployment.
  - Use descriptive naming for Topology Policy Groups for easier management.
  - Combine topology design with application-aware routing to optimize performance.
  - Monitor link health and adjust topology policies as site roles change.

Lab 5: Creating Topologies

- Create and deploy a Full Mesh topology for all branch sites in a single VPN.
- Configure a Hub-and-Spoke topology for centralized security inspection.
- Design a Custom topology connecting regional hubs with selective branch interconnections.
- Validate topology behavior and routing paths using policy visualization and topology overlays.

Module 7: UX1.0 and 2.0 Topology Coexistence

- Coexistence Scenarios
  - Partial Upgrade Environments: Some WAN Edge devices are managed using UX 2.0 Configuration & Policy Groups, while others remain on UX 1.0 centralized templates and policies.

    - Phased Rollout Approach: Gradual migration from UX 1.0 to UX 2.0 where site cutovers are scheduled based on priority or readiness.
- Policy Compatibility Considerations
    - UX 2.0 Policy Groups (Application, Security, Topology) replace multiple UX 1.0 control policy constructs.
    - Only one active topology definition can be in effect-either via UX 2.0 Topology policies or UX 1.0 centralized control policies.
    - Security and application-aware routing rules created in UX 1.0 will continue to apply to devices still managed under that interface.
- Operational Impact
    - Device groups managed in UX 2.0 cannot consume or apply UX 1.0 centralized control policies.
    - Monitoring remains unified; topology and alarms display all devices, regardless of management interface.
    - Feature parity differences-some features may be available only in UX 2.0 or still require UX 1.0 until fully migrated.
- Configuration & Deployment Workflows
    - Keep configuration and policy assignments consistent between UX 1.0 and UX 2.0 to avoid policy gaps.
    - Use device inventory tags to distinguish management method and prevent accidental cross-application of incompatible policy sets.
    - Maintain version alignment on WAN Edge software to minimize unexpected behavior.
- Best Practices
    - Plan coexistence periods to be as short as operationally possible.
    - Test new UX 2.0 policies in a lab before applying them to production devices in mixed-mode environments.
    - Document which devices and sites are managed under each interface version for clear operational handoff.
    - Use the UX 2.0 topology view for network-wide visibility, even when some policies are still enforced via UX 1.0.

Lab 6: UX 2.0 Topology Coexistence

- Identify devices managed under UX 1.0 and UX 2.0 within the same environment.
- Create a UX 2.0 Policy Group for a set of branch devices while leaving data center devices under UX 1.0 centralized control policy.
- Validate that topology view accurately reflects both UX 1.0 and UX 2.0 managed segments.
- Apply troubleshooting steps for a mixed-mode policy conflict and resolve by updating the correct interface version.

Module 8: Migrating from UX 1.0 to UX 2.0

- Pre-Migration Preparation
    - Version Compatibility: Ensure WAN Edge devices and controllers are running supported software versions for UX 2.0 features.
    - Inventory Audit: Document devices, templates, policies, and feature usage in UX 1.0.
    - Feature Readiness Check: Verify that all necessary features exist in UX 2.0 or have acceptable workarounds.
    - Stakeholder Alignment: Inform operational teams of expected changes in workflows, interfaces, and policy management.
- Migration Strategy
    - Phased Migration: Migrate devices in stages, starting with a pilot group to validate the process.
    - Parallel Coexistence: Maintain some devices in UX 1.0 during early phases for operational continuity.
    - Policy Mapping: Translate centralized control policies from UX 1.0 into Policy Groups in UX 2.0 (Application, Security, Topology).

    - Configuration Translation: Move from device templates in UX 1.0 to Configuration Groups in UX 2.0, reusing Feature Profiles and Parcels where possible.
- Execution Workflow
    - Backup UX 1.0 configuration data and policies.
    - Create equivalent Configuration and Policy Groups in UX 2.0.
    - Assign devices to new groups and deploy.
    - Monitor deployment success and validate connectivity.
- Post-Migration Validation
    - Confirm policy enforcement using the UX 2.0 topology and policy visualization tools.
    - Check device health, alarms, and performance metrics.
    - Validate user experience for critical applications.
- Rollback Plan
    - Maintain UX 1.0 configurations and policies for rapid redeployment if needed.
    - Establish a time-bound rollback window for each migration batch.
    - Clearly document triggers for rollback (e.g., policy failure, routing instability).
- Best Practices
    - Always run a small-scale migration in a lab or low-risk site before production rollout.
    - Keep policy and configuration naming conventions consistent across UX 1.0 and UX 2.0 during transition for easier tracking.
    - Document every step and keep change logs for future audits.
    - Involve both operations and engineering teams in post-migration verification.

Lab 7: Migrating from UX 1.0 to UX 2.0

- Identify devices and policies ready for migration from UX 1.0 to UX 2.0.
- Translate a UX 1.0 centralized control policy into a UX 2.0 Policy Group.
- Create a Configuration Group equivalent to an existing UX 1.0 device template and assign it to a test device.
- Perform a simulated migration, validate policy and configuration deployment, and test rollback.

Module 9: Monitoring & Troubleshooting the SD-WAN UX 2.0 Solutions

- Monitoring in UX 2.0
    - Dashboard Widgets: Device health, link status, alarms, application performance, and deployment status.
    - Real-Time Topology View: Visual network health, link quality overlays, and policy enforcement points.
    - Historical Playback: Time-based topology replay for incident analysis.
    - Alarm Management: Severity-based filtering, acknowledgment, and correlation.
- Performance Analysis
    - WAN link quality metrics (loss, latency, jitter).
    - Application-aware monitoring for critical business apps.
    - Device CPU, memory, and interface utilization statistics.
- Troubleshooting Tools
    - Policy Visualization: Validate policy application and identify mismatches.
    - Device Drill-Down: View running configuration, logs, and event history directly from UX 2.0.
    - Ping and Trace Tools: Run from vManage to specific devices for connectivity verification.
    - Configuration History: Compare revisions and roll back if needed.
- Common Issue Scenarios
    - Policy conflicts after migration from UX 1.0 to UX 2.0.
    - Device configuration drift due to manual changes.
    - Topology inconsistencies caused by outdated inventory data.
    - Link degradation and packet loss impacting application SLAs.
- Structured Troubleshooting Workflow
    - Detect: Identify the issue through alarms or user reports.

    - Isolate: Use topology and monitoring tools to locate the root cause.
    - Remediate: Apply configuration or policy adjustments.
    - Validate: Confirm resolution through monitoring and policy visualization.
- Best Practices
    - Enable historical playback for incident review to catch intermittent issues.
    - Standardize alarm thresholds across the network for consistent monitoring.
    - Tag devices and sites for quicker filtering during troubleshooting.
    - Use the Modify stage to test fixes in a non-disruptive way before deploying.

Lab 8: Monitoring & Troubleshooting the SD-WAN UX 2.0 Issues

- Use the dashboard to identify devices with critical alarms.
- Navigate the topology view to locate a device experiencing packet loss and review link metrics.
- Use policy visualization to verify if traffic steering rules are being applied correctly.
- Run a troubleshooting workflow to resolve a simulated application performance issue.