

IBM Certified Deployment Professional — Security Verify Access V10.0

OEM: IBM • Duration: 5 Days (40 hrs) • Code: C1000-129

COURSE MODULES & TOPICS

Section 1: Planning (12%)

- Conduct planning workshops
- Identify feature requirements
- Plan firmware upgrade cycle
- Perform solution sizing
- Assess access control requirements
- Assess log retention requirements
- Assess federated single sign-on requirements

Section 2: Architecture and Design (15%)

- Select deployment patterns and topology
- Design High Availability and Disaster Recovery architecture
- Design deployment process (automated or manual)
- Identify network requirements
- Establish backup procedures
- Determine appropriate junction type
- Identify required authentication methods

Section 3: Installation (13%)

- Find and download software and updates
- Create virtual machine
- Prepare user registry and database(s)
- Deploy Security Verify Access containers
- Activate required offerings and install the support license
- Perform network configuration
- Import personal and signer certificates

Section 4: Configuration (16%)

- Configure cluster
- Configure base runtime component

- Integrate federated directories
- Configure reverse proxy instance
- Configure authorization server
- Configure LMI external authentication and authorization
- Configure multi-factor authentication (MFA)
- Configure SCIM
- Configure API protection (OAUTH/OIDC)
- Configure auditing

Section 5: System Integration (16%)

- Configure Junction
- Protect API endpoints accessed by API clients
- Integrate with federated single sign-on partners
- Configure desktop SSO (SPNEGO)
- Configure token authentication
- Setup monitoring framework
- Configure external authentication interface
- Integrate with SIEM systems

Section 6: Advanced Customization (18%)

- Implement a context-based access control policy
- Create risk profile
- Implement identity mapping
- Author custom policy information point (PIP)
- Configure and customize a user self-care flow
- Create JavaScript authentication mechanism
- Create HTTP transformation rules
- Implement OAUTH/OIDC customization
- Configure device registration (Fingerprint)
- Configure single sign-on using Federation STS

Section 7: Testing, Troubleshooting, and Maintenance (10%)

- Apply interim fixes
- Apply appliance firmware updates
- Resolve common problems
- Prepare backup storage system
- Perform tuning
- Configure logging and tracing
- Engage with IBM Support