DEPLOY, CONFIGURE AND MANAGE CISCO DUO

Version 2.0

Blue River Education GmbH, Schoßbachstrasse 20c, 9400 Wolfsberg, Austria
Company Register FN 429823, VAT ID ATU69349314

https://br-experts.eu/
office@blueriveredu.com

1 Course Overview

In this 3-day course you will learn to deploy, configure and manage Cisco Duo. In the present scenario the workforce of any company can connect from anywhere and everywhere using any device. So, companies must ensure that all the company assets are protected. Cisco Duo fits into a zero-trust security model assuring proper authentication of users and devices and continuously monitors each access attempt, ensuring that all the users accounts, devices and applications are protected from unauthorized access company wide.

2 Who Should Attend

- Network Administrators
- Network Engineers
- Sales Engineers
- System Engineers
- Anyone who wants to learn about Multi-Factor Authentication (MFA)

3 Prerequisites

Before taking this course, it would be good to have exposure to the following:

- Network Fundamentals
- Network Security Fundamentals
- Endpoint Agents

4 Why Attend a Blue River Experts Course

Our courses are not delivered by instructors but by consulting system engineers who have vast experience regarding real life design, deployment, and troubleshooting of actual customer installations. Besides delivering courses, our engineers usually design and deploy large enterprise solutions or perform real world POVs (proof of value) and POCs (proof of concept) for large customers. We are often requested and contracted by product vendors to help customers make buying decisions based on their particular use case. This allows us to discuss real world use cases, designs, and operational situations with our students.

If you would like to get educated by experts who will explain to you the whole life cycle from day 0 to day 2 as they have comprehensive knowledge from having written numerous business requirements documents, customer requirements documents, high level design and detailed design documents and having deployed and troubleshooted many customer installations then you should choose to attend one of our courses.

5 Course Objectives

After completing this course, students will be able to:

- Describe the different authentication methods
- Perform endpoint and user enrolment
- Work with the Duo admin portal
- Protect applications
- Describe and perform directory synchronization
- Describe and configure Duo SSO
- Describe Duo access gateway and Duo access features
- Describe and implement trusted endpoints
- Describe and perform various management functions
- Explain various Duo use cases

6 Course Details

6.1 Fundamentals of Authentication Methods

- What is Authentication?
- Different authentication methods
- Two-factor (2FA) authentication and beyond (MFA)
- Why do you need 2FA?
- 2FA/ MFA using Cisco Duo

6.2 Getting started with Duo MFA

- Overview of Duo Security
- Different Licensing Models (MFA, Access and Beyond)
- Authenticating (Duo Prompt, Duo Universal Prompt, Duo Central)
- Endpoint and User Enrolment

6.3 Duo Administration Overview

- Accessing Duo Admin Portal
- Administrator and Users Account Setup
- Dashboard and Navigation
- Viewing Information and Reports

6.4 Enrolling Users

- Automatic
- Self-Enrolment
- Manual Enrolment
- Activating Duo Mobile

6.5 Protecting Applications

- Application Options
- New and Existing Applications
- Application Updates
- Universal Prompt Activation
- View your applications
- Remove an application

6.6 Duo Directory Sync

- Overview of Directory Sync
- Azure AD Synchronization
- Active Directory Synchronization
- OpenLDAP Synchronization

6.7 Duo SSO/ SAML

- Duo SSO/ SAML overview
- Prerequisites
- Enabling Duo SSO
- Configuring the Authentication Source
- Creating a Cloud Application
- Duo Central

6.8 Duo Access Gateway (DAG)

- DAG Overview
- DAG for Windows
- DAG for Linux
- DAG and Universal Prompt

6.9 Duo Access Features

- Access Overview
- Policy and Control
- Device Insight
- Endpoints Insight
- Health monitoring
- Trust monitoring

6.10 Duo Beyond Features

- Trusted Endpoints
- Duo Network Gateway

6.11 Trusted Endpoints

- Overview of Trusted Endpoints
- Device Health Verification
- Duo Mobile Verification
- Certificate Verification
- Best Practices - Implementing Trusted Endpoints
- Applying the Trusted Endpoints Policy
- Monitoring Trusted Endpoints
- Controlling Application Access for Trusted Endpoints

6.12 Operations and Management

- Changing Settings
- End user and Admin Management
- Device Management
- Using groups
- Usability enhancements
- Software Downloads and Updates

6.13 Remote Access & VPN Use-Cases

- Duo Network Gateway
- Cisco AnyConnect VPN with ASA or Cisco Secure Firewall
- Duo 2FA for Meraki Client VPN

6.14 Common Use Cases

- Duo Single Sign-On
- Microsoft RDP
- Web Applications
- Identity Providers (Cisco Identity Services Engine)

7 Lab Exercises

7.1 Setting up student's administrative account

7.2 Admin login settings / review settings

7.3 Configuring a group

7.4 Users' enrollment

- User's self-enrollment
- Bulk users' enrollment (optional)
- Import users
- Active Directory Sync, Authentication Proxy Installation & Configuration
- Deleting a user

7.5 Protecting "Cisco RADIUS VPN" – Cisco ASA VPN + DUO + AD

7.6 Configuring SSO and protecting Meraki dashboard

- SSO configuration
- Creating a Meraki Dashboard account
- Protecting a Meraki application
- Duo Central configuration

7.7 Duo Network Gateway Setup

- Initial configuration for Duo Network Gateway
- Protecting Duo Network Gateway SSO
- Configuring authentication source for Duo Network Gateway login

7.8 Setup Duo Network Gateway Web Application

- Protecting a Duo Network Gateway – Web Application
- Configuring Duo Network Gateway Web App tile
- Test Web Application from Duo Network Gateway

7.9 Setup Duo Network Gateway SSH Application

- Protecting Duo Network Gateway SSH application
- Configuring Duo Network Gateway SSH tile
- Test your internal SSH protected application

7.10 Trusted Endpoints & Duo Health

- Integrate Trusted Endpoints
- Configuring policies
- Associating a policy to a protected application
- Test the application where the policy is applied
- Reports for auditing
- Configure Health application
- Test the flow for visibility
- Reporting
- Configure policy with enforcement
- Test with endpoint for enforcement