



Module Specification

Directory Services and Policy Management

Version: 2027-28, v1.0, 20 Jan 2025

Contents

Module Specification	1
Part 1: Information	2
Part 2: Description	2
Part 3: Teaching and learning methods	4
Part 4: Assessment.....	5
Part 5: Contributes towards	7

Part 1: Information

Module title: Directory Services and Policy Management

Module code: UFCEJ5-30-3

Level: Level 6

For implementation from: 2027-28

UWE credit rating: 30

ECTS credit rating: 15

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: This module gives students the opportunity to explore the technology used to deploy and manage directory services and complex domain management systems to facilitate centralised device management, software deployment, user administration and information security.

This module will be supported by practical labs and test environments allowing

students to design and test a range of technologies to appreciate their merits and limitations.

Features: Not applicable

Educational aims: This module will enable you to design and develop an directory services solution to facilitate centralised network management and information assurance.

The overall focus of this module is on the services and capabilities that directory services solutions enable in an organisational context and prepare students for a role as network administrator, compliancy and information security assurance.

Key topics will include

- Centralised domain management
- Device management
- User management, permissions and access control
- Software management and deployment
- Cloud, on premise and hybrid domain management solutions
- Compliancy and information security

Outline syllabus: Standalone clients vs client-server networks and importance and limitations of user and device management to facilitate audit, compliancy, and information security requirements on cooperate networks.

Device management: Domain deployment, enrolling devices, group management, roaming devices

Directory management: Operational groups, linked policies, policy inheritance

Group policy configuration and best practice

Software management: Software packaging, testing and deployment, licensing considerations.

Directory solutions and contemporary third-party tools.

Domain configuration (eg, server, DHCP, DNS requirements)

File storage and management, roaming profiles, file access and permissions.

Domain administration: on-premise, cloud and hybrid management.

Multi-site/multi-domain solutions (Eg domain tree, forest)

Key legislation and information security standards, e.g. software licensing and contemporary frameworks (for instance, Cyber Essentials, ISO27001 and the GDPR).

Part 3: Teaching and learning methods

Teaching and learning methods: This module will be delivered through introductory lectures covering the fundamentals and technical underpinning of the module. This progresses onto practical delivery through a series of lessons, workshops and practical tasks in a Network Lab. This will develop the experience and facilitate the module assessment.

The emphasis of this module will be on network management/administration via directory services. Labs may use virtual environments.

Opportunities for feedback and time to develop hands-on experience with a range of technologies and operating systems will exist throughout the module.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Evaluate the key technologies available to manage devices, software and users over large networks.

MO2 Configure, test and deploy a directory services solution.

MO3 Design, develop and document a secure directory services solution to manage a range of devices and software deployments.

MO4 Deploy and test file management controls to ensure information security.

Hours to be allocated: 300

Contact hours:

Independent study/self-guided study = 228 hours

Face-to-face learning = 72 hours

Reading list: The reading list for this module can be accessed at [readinglists.uwe.ac.uk](https://rl.talis.com/3/uwe/lists/99BDA692-11A5-57E0-2152-FCAA3A8DF919.html) via the following link <https://rl.talis.com/3/uwe/lists/99BDA692-11A5-57E0-2152-FCAA3A8DF919.html>

Part 4: Assessment

Assessment strategy: This module consists of two assessments to cover both the practical application and rationale of key services and technologies.

The three hour, Time Constrained Assessment will assess students' ability to apply domain controls to a given system in a Network Lab environment, complemented by written questions and answers addressing the key technologies applied.

The final assessment requires students to design, develop and document a compressive directory services solution to demonstrate the practical setup and configuration of the tools and controls detailed in the module outcomes. The final documentation/report (2000 words) will be submitted alongside supporting evidence taken from the practical lab.

The resit opportunity will follow the same format as the first sit, with the option for a re-work of the portfolio if appropriate.

Assessment tasks:

Portfolio (First Sit)

Description: Students will be required to design and develop a secure directory services solution for a complex network scenario comprising multiple devices, users and groups. Students will be required to document the completed system with supporting evidence (2000 words)

Weighting: 75 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO2, MO3, MO4

In-class test (First Sit)

Description: Students will be required to complete a three-hour, in class Time Constrained Assessment in which they will be required to complete a series of short practical tasks focusing on securing a directory-services configured solution and written questions addressing the technical understanding of key technologies.

Weighting: 25 %

Final assessment: No

Group work: No

Learning outcomes tested: MO1

Portfolio (Resit)

Description: Students will be required to design and develop a secure directory services solution for a complex network scenario comprising multiple devices, users and groups. Students will be required to document the completed system with supporting evidence (2000 words)

Given the size and complexity of the practical component, a re-working may be considered for this assessment if appropriate.

Weighting: 75 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO2, MO3, MO4

In-class test (Resit)

Description: Students will be required to complete a three-hour, in class Time Constrained Assessment in which they will be required to complete a series of short practical tasks focusing on securing a directory-services configured solution and written questions addressing the technical understanding of technologies in the module syllabus.

Weighting: 25 %

Final assessment: No

Group work: No

Learning outcomes tested: MO1

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security and Networking {Top-up} [UCW] BSc (Hons) 2027-28