



**Australian Government**

**Assessment Requirements for ICTNWK538  
Install and maintain valid authentication  
processes**

**Release: 1**

# Assessment Requirements for ICTNWK538 Install and maintain valid authentication processes

## Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

## Performance Evidence

The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to:

- design and deploy authentications solutions to a medium-sized business technology environment.

In the course of the above, the candidate must:

- configure authentication software and tools
- align authentication processes to organisational requirements and industry standard best practices
- document work plans and processes.

## Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including knowledge of:

- problems and challenges associated with organisational authentication issues, including resource accounting through authentication
- industry standard virtual private network (VPN) issues, including:
  - quality of service (QoS) considerations
  - bandwidth
  - dynamic security environment
  - function and operation of VPN concepts
- authentication adaptors, including biometric authentication adaptors
- digital certificates, including:
  - VeriSign
  - X.509
  - SSL

- function and operation of authentication controls and protocols including:
  - passwords and personal identification numbers (PINs)
  - smart cards biometric devices
- network authentication services including:
  - Kerberos
  - NT LAN Manager (NTLM)
- features of common password protocols, including:
  - challenge handshake authentication protocol (CHAP)
  - challenge phrases
  - password authentication protocol (PAP)
  - remote authentication dial-in user service (RADIUS) authentication
- principles of security tokens.

## Assessment Conditions

Skills in this unit must be demonstrated in a workplace or simulated environment where the conditions are typical of those in a working environment in this industry.

- a site or prototype where network authentication may be implemented and managed
- network support tools currently used in industry
- organisational security policies related to authentication
- manufacturers recommendations
- current authentication standards, including biometric authentication adaptors.

Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

## Links

Companion Volume Implementation Guide is found on VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>