



Australian Government

ICTNWK503 Install and maintain valid authentication processes

Release: 1

ICTNWK503 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 1.0.

Application

This unit describes the skills and knowledge required to design, develop, install and maintain authentication processes to reduce the vulnerability of the system.

It applies to individuals working as middle managers such as information security managers, network engineers or security analysts, who are responsible for implementing and monitoring the organisational security management system.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Unit Sector

Networking

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
1. Determine authentication requirements	1.1 Determine user and enterprise security requirements with reference to enterprise security plan 1.2 Identify and analyse authentication options according to user and enterprise requirements 1.3 Select the most appropriate authentication and authorisation processes
2. Configure authentication software or tools	2.1 Create an authentication realm and reuse as required to protect different areas of server 2.2 Add users and authorisation rules to new realm according to business needs

ELEMENT	PERFORMANCE CRITERIA
	2.3 Describe user attributes and user attribute set-up 2.4 Set up an authentication filter and authorisation parameters on the appropriate server according to business requirements
3. Apply authentication methods	3.1 Develop or obtain authentication protocols as required 3.2 Develop and distribute related methods to users according to business need 3.3 Brief user on authentication system and their responsibilities according to enterprise security plan 3.4 Apply authentication system to network and user according to system product requirements 3.5 Record and store permission and configuration information in a secure central location
4. Monitor authentication system	4.1 Review the authentication system according to user and enterprise security and quality of service requirements 4.2 Ensure ongoing security monitoring, using incident management and reporting processes, according to enterprise security plan 4.3 Adjust authentication system if required

Foundation Skills

This section describes language, literacy, numeracy and employment skills incorporated in the performance criteria that are required for competent performance.

Skill	Performance Criteria	Description
Reading	1.1, 1.2, 3.3, 4.2	Gathers, interprets and analyses technical data to determine requirements according to user and enterprise plans
Writing	2.3, 3.1, 3.2, 3.5	Prepares workplace documentation that incorporates an evaluation of technical information and specialised and cohesive language in a format and style appropriate for a specific audience
Oral Communication	1.2, 3.1-3.3, 4.2	- Uses active listening, observational and questioning techniques in order to identify information and confirm, clarify or revise understanding - Initiates and contributes to a range of formal and

		informal conversations relevant to role, responding, clarifying, explaining and expanding on information as required
Navigate the world of work	1.1, 3.3	Recognises and follows explicit and implicit protocols, and meets expectations associated with own role
Get the work done	1.1, 1.3, 2.1, 2.2, 2.4, 3.4, 3.5, 4.1-4.3	- Reflects on the ways in which digital systems and tools are used or could be used to achieve work goals and begins to recognise strategic and operational applications - Uses digital technologies and systems safely and securely when implementing and monitoring a system with a growing awareness of the permanence and transparency of all activities - Uses a combination of formal, logical planning processes and an increasingly intuitive understanding of context to plan control methods and systems processes - When dealing with complex issues such as authentication failure and security incidents may use intuition to identify the general problem area, switching to analytical processes to clarify goals and key issues and using lateral thinking processes to generate possible solutions - Makes decisions in relatively complex situations, taking a range of factors into consideration

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTNWK503 Install and maintain valid authentication processes	ICANWK503A Install and maintain valid authentication processes	Updated to meet Standards for Training Packages	Equivalent unit

Links

Companion Volume implementation guides are found in VETNet -

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

Assessment Requirements for ICTNWK503 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 1.0.

Performance Evidence

Evidence of the ability to:

- design and deploy authentications solutions to the business technology environment and business needs
- configure authentication software or tools
- monitor and test authentication process after implementation
- ensure authentication solutions are current.

Note: If a specific volume or frequency is not stated, then evidence must be provided at least once.

Knowledge Evidence

To complete the unit requirements safely and effectively, the individual must:

- summarise the problems and challenges dealing with organisational authentication issues, including resource accounting through authentication
- discuss common virtual private network (VPN) issues, including:
 - quality of service (QoS) considerations
 - bandwidth
 - dynamic security environment
 - function and operation of VPN concepts
- outline authentication adaptors
- summarise biometric authentication adaptors
- summarise digital certificates, such as VeriSign, X.509, and SSL
- explain the function and operation of authentication controls including:
 - passwords
 - personal identification numbers (PINs)
 - smart cards

- biometric devices
- other authentication protocols
- outline network authentication services, such as Kerberos and NT LAN Manager (NTLM)
- summarise the features of common password protocols, such as:
 - challenge handshake authentication protocol (CHAP)
 - challenge phrases
 - password authentication protocol (PAP)
 - remote authentication dial-in user service (RADIUS) authentication
- describe the principles of security tokens.

Assessment Conditions

Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the network industry, and include access to:

- 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 must satisfy NVR/AQTF assessor requirements.

Links

Companion Volume implementation guides are found in VETNet -

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