

TECHNICAL PRODUCT BRIEF

Wireless penetration testing

Validate the security boundary around wireless access.

Why customers use this service

Test corporate, guest and representative wireless networks to identify weak authentication, isolation, management and trust paths into connected environments.

What we assess

Network discovery	Authorised wireless networks, broadcast behaviour and unexpected exposure.
Authentication	Enterprise, personal and captive-portal access controls.
Client isolation	Whether connected devices can reach each other unexpectedly.
Network separation	Boundaries between guest, corporate and sensitive environments.
Management security	Administrative interfaces and wireless infrastructure controls.
Rogue access risks	Client trust and resistance to misleading or unauthorised access points.
Encryption and legacy modes	Protocol choices that weaken confidentiality or access control.

Engagement outcome

A prioritised report with validated wireless access and trust findings, evidence, remediation guidance and retest results.

[How the engagement works](#)

How we test or review

Damocles observes authorised radio environments onsite, joins approved SSIDs with supplied clients, and validates isolation and post-connect paths against configuration evidence. Radio observations are location and time bound, and production-impacting deauthentication is excluded unless separately authorised.

Testing and review perspectives

Onsite radio and unauthenticated wireless assessor

Surveys approved locations for SSIDs, channels, encryption and authorised lookalike conditions without joining protected networks.

Included when: Used for radio discovery, advertised security and location-specific exposure.

Access: Site access, approved locations, SSID inventory, testing window and radio constraints.

Limitations: Observations are limited by location, time, equipment and signal propagation.

Supplied corporate or guest wireless client

Joins approved SSIDs with supplied credentials or certificates and tests isolation and post-connect access.

Included when: Used when authenticated corporate or guest behaviour is included.

Access: A test device, onboarding material, credentials and expected network access.

Limitations: Represents only the supplied client, identity, SSID and location.

Wireless configuration and segmentation reviewer

Reviews controller, access-point, identity and network policy and correlates it with radio and connectivity results.

Included when: Used when wireless configuration and downstream segmentation evidence is available.

Access: Controller exports, authentication policy, VLAN mapping, certificates and flow expectations.

Limitations: Configuration alone does not prove RF coverage or live enforcement.

Customer access or evidence typically required

Site access, approved locations, SSID inventory, testing window and radio constraints.; A test device, onboarding material, credentials and expected network access.; Controller exports, authentication policy, VLAN mapping, certificates and flow expectations.

What you receive

A prioritised report with validated wireless access and trust findings, evidence, remediation guidance and retest results.

Detailed technical coverage

Approved SSIDs and locations

What is assessed	Damocles surveys each approved site and location for SSIDs, BSSIDs, channels, signal presence and advertised security and reconciles results with the authorised inventory.
Perspective / access	Onsite radio and unauthenticated wireless assessor. Approved ranges, names, locations and the expected asset or interface inventory.
Evidence	A discovered-item register with address, service, version or location and reconciliation status.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed for customer-owned ranges, names, locations or interfaces listed in the authorised inventory.
Limitations	Discovery is point-in-time and cannot establish ownership or absence outside the approved inventory; intrusive enumeration stops at the agreed boundary.

Authentication modes

What is assessed	Damocles validates applicable WPA2, WPA3, enterprise or personal authentication modes using supplied test clients and identities.
Perspective / access	Supplied corporate or guest wireless client. Assessment requires approved site access, locations, SSIDs, test clients, onboarding material and controller or network evidence, selected specifically for authentication modes.
Evidence	Evidence records the SSID, BSSID, radio, authentication, client-isolation or post-connect result relevant to authentication modes.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Authentication modes when the wireless feature is present at an approved location.
Limitations	The conclusion is limited to the sampled authentication modes; radio results are location and time bound; disruptive RF actions require separate written authority.

Certificate and credential onboarding

What is assessed	Damocles follows certificate and credential enrolment, renewal, storage and removal on an approved client and reviews the associated identity policy.
Perspective / access	Onsite radio and unauthenticated wireless assessor. Assessment requires approved site access, locations, SSIDs, test clients, onboarding material and controller or network evidence, selected specifically for certificate and credential onboarding.
Evidence	Evidence records the SSID, BSSID, radio, authentication, client-isolation or post-connect result relevant to certificate and credential onboarding.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Certificate and credential onboarding when the wireless feature is present at an approved location.
Limitations	The conclusion is limited to the sampled certificate and credential onboarding; radio results are location and time bound; disruptive RF actions require separate written authority.

Encryption configuration

What is assessed	Damocles inspects negotiated encryption, protected-management settings and controller policy and performs only authorised downgrade checks.
Perspective / access	Wireless configuration and segmentation reviewer. Current configuration export or read-only access, diagrams, owners and representative validation endpoints.
Evidence	Configuration excerpts, object or rule identifiers and observed validation results.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed when current configuration evidence and a representative endpoint or device are included in the review.
Limitations	A configuration snapshot cannot prove continuous enforcement across excluded nodes; validation avoids changes unless implementation work is authorised.

Client isolation

What is assessed	Damocles attempts direct client-to-client communication between supplied clients on the same approved SSID.
Perspective / access	Onsite radio and unauthenticated wireless assessor. Assessment requires approved site access, locations, SSIDs, test clients, onboarding material and controller or network evidence, selected specifically for client isolation.
Evidence	Evidence records the SSID, BSSID, radio, authentication, client-isolation or post-connect result relevant to client isolation.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Client isolation when the wireless feature is present at an approved location.
Limitations	The conclusion is limited to the sampled client isolation; radio results are location and time bound; disruptive RF actions require separate written authority.

Guest isolation

What is assessed	Damocles attempts approved guest-to-corporate, guest-to-management and guest-to-peer paths after connection.
Perspective / access	Onsite radio and unauthenticated wireless assessor. Assessment requires approved site access, locations, SSIDs, test clients, onboarding material and controller or network evidence, selected specifically for guest isolation.
Evidence	Evidence records the SSID, BSSID, radio, authentication, client-isolation or post-connect result relevant to guest isolation.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Guest isolation when the wireless feature is present at an approved location.
Limitations	The conclusion is limited to the sampled guest isolation; radio results are location and time bound; disruptive RF actions require separate written authority.

Rogue and lookalike conditions

What is assessed	Damocles observes and, where expressly authorised, establishes controlled rogue or lookalike conditions to test user and control response.
Perspective / access	Onsite radio and unauthenticated wireless assessor. Assessment requires approved site access, locations, SSIDs, test clients, onboarding material and controller or network evidence, selected specifically for rogue and lookalike conditions.

Evidence	Evidence records the SSID, BSSID, radio, authentication, client-isolation or post-connect result relevant to rogue and lookalike conditions.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Rogue and lookalike conditions when the wireless feature is present at an approved location.
Limitations	The conclusion is limited to the sampled rogue and lookalike conditions; radio results are location and time bound; disruptive RF actions require separate written authority.

Downgrade conditions

What is assessed	Damocles checks whether authorised clients can be induced to use weaker advertised or negotiated security without disruptive RF activity.
Perspective / access	Onsite radio and unauthenticated wireless assessor. Assessment requires approved site access, locations, SSIDs, test clients, onboarding material and controller or network evidence, selected specifically for downgrade conditions.
Evidence	Evidence records the SSID, BSSID, radio, authentication, client-isolation or post-connect result relevant to downgrade conditions.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Downgrade conditions when the wireless feature is present at an approved location.
Limitations	The conclusion is limited to the sampled downgrade conditions; radio results are location and time bound; disruptive RF actions require separate written authority.

Network segmentation

What is assessed	Damocles maps SSIDs to VLANs or policy segments and validates representative allowed and denied post-association paths.
Perspective / access	Onsite radio and unauthenticated wireless assessor. Named source and destination test points, expected flow matrix and a safe test window.
Evidence	Source-to-destination results linked to rule, route or boundary evidence.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Performed when both ends of the network path and the enforcing device are owned or expressly authorised for testing.
Limitations	Results cover the tested source, destination, protocol and route; testing stops on instability and does not authorise third-party or denial-of-service activity.

Post-connect access

What is assessed	Damocles tests the actual DNS, internet, internal and management access assigned to supplied corporate or guest clients.
Perspective / access	Supplied corporate or guest wireless client. Assessment requires approved site access, locations, SSIDs, test clients, onboarding material and controller or network evidence, selected specifically for post-connect access.
Evidence	Evidence records the SSID, BSSID, radio, authentication, client-isolation or post-connect result relevant to post-connect access.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Post-connect access when the wireless feature is present at an approved location.

Limitations	The conclusion is limited to the sampled post-connect access; radio results are location and time bound; disruptive RF actions require separate written authority.
--------------------	--

Onsite and radio constraints

What is assessed	Damocles records site position, antenna, channel, interference and signal limitations for every radio observation.
Perspective / access	Onsite radio and unauthenticated wireless assessor. Assessment requires approved site access, locations, SSIDs, test clients, onboarding material and controller or network evidence, selected specifically for onsite and radio constraints.
Evidence	Evidence records the SSID, BSSID, radio, authentication, client-isolation or post-connect result relevant to onsite and radio constraints.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Onsite and radio constraints when the wireless feature is present at an approved location.
Limitations	The conclusion is limited to the sampled onsite and radio constraints; radio results are location and time bound; disruptive RF actions require separate written authority.

Deauthentication and production safety

What is assessed	Damocles documents deauthentication and disruptive RF exclusions and performs such activity only with written authority, a controlled window and stopping criteria.
Perspective / access	Supplied corporate or guest wireless client. Assessment requires approved site access, locations, SSIDs, test clients, onboarding material and controller or network evidence, selected specifically for deauthentication and production safety.
Evidence	Evidence records the SSID, BSSID, radio, authentication, client-isolation or post-connect result relevant to deauthentication and production safety.
References	Technical Guide to Information Security Testing and Assessment SP 800-115
Applicability	Applies to Deauthentication and production safety when the wireless feature is present at an approved location.
Limitations	The conclusion is limited to the sampled deauthentication and production safety; radio results are location and time bound; disruptive RF actions require separate written authority.

Methodologies and standards

Technical Guide to Information Security Testing and Assessment SP 800-115 — Uses NIST SP 800-115 guidance to plan, execute, analyse and report the authorised procedure.

Information Security Manual June 2026 — Provides ASD ISM control context only for the declared mapping and observed behaviour.

Common Weakness Enumeration 4.20 — Classifies confirmed weakness types using CWE 4.20.

Common Vulnerability Scoring System 4.0 — Calculates technical severity and records a CVSS 4.0 vector separately from customer impact.

Standards and control mappings

Security and Privacy Controls for Information Systems and Organizations Release 5.2.0 — contextual

References: Framework-level mapping

Assessed: The engagement produces point-in-time technical evidence about the configured and observed security behaviour within the authorised Wireless penetration testing scope.

Evidence: Coverage status, procedure results and findings can inform the customer's control assessment and risk treatment records.

Applicability: Framework-level context is provided when the customer uses NIST SP 800-53 to organise its security control program.

Limitations: No individual NIST control is published as verified; organisational implementation, continuous operation, governance and complete catalogue coverage remain outside the engagement.

What you receive: report and evidence

Authorised scope and rules of engagement

Records authorised scope and rules of engagement produced from the authorised Wireless penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Coverage matrix

Records coverage matrix produced from the authorised Wireless penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Retest and residual-risk record

Records retest and residual-risk record produced from the authorised Wireless penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

SSID and authentication inventory

Records ssid and authentication inventory produced from the authorised Wireless penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Radio and client-isolation results

Records radio and client-isolation results produced from the authorised Wireless penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Post-connect reachability record

Records post-connect reachability record produced from the authorised Wireless penetration testing work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Scope and safety limitations

- Only expressly authorised assets, identities, locations and activities are assessed.
- Higher-risk, disruptive, destructive and third-party activity requires separate written authority.
- Point-in-time evidence cannot establish continuous operation or conditions outside the engagement.

Assurance boundary

Damocles maps assessed coverage and findings to agreed security frameworks and control objectives. This provides traceable technical evidence that may support risk, assurance and audit activities. A penetration test does not by itself certify an organisation, establish complete compliance with a framework or confirm the effectiveness of controls outside the authorised scope.

Review metadata

Owner: Technical Assurance

Last reviewed: 2026-08-10

Next review due: 2026-12-10

Scope this engagement with Damocles Security
damocles.com.au/contact

Assurance boundary

Damocles maps assessed coverage and findings to agreed security frameworks and control objectives. This provides traceable technical evidence that may support risk, assurance and audit activities. A penetration test does not by itself certify an organisation, establish complete compliance with a framework or confirm the effectiveness of controls outside the authorised scope.

This brief supports engagement scoping. The authorised scope, rules of engagement and applicable agreement govern delivery.