JUNIPER ODYSSEY ACCESS CLIENT FIPS VERSION 4.56

Product Description

Juniper Odyssey Access Client (hereafter referred to as 'Juniper Odyssey' or 'the product') is a software-only access client for wireless and wired 802.1X networks. The product allows supplicants to establish communication with a private network. IP packets passing between the supplicant and the private network are encrypted.

Evaluation Scope

The scope of the DSD Cryptographic Evaluation (DCE) included the following functionality:

- Authentication
- Data confidentiality
- Data integrity

Common Criteria Certification – Summary

The product was found to meet the requirements of the Common Criteria (CC) evaluation assurance level EAL3+.

DSD Findings and Recommendations

DSD performed a cryptographic evaluation on the product in addition to the Common Criteria evaluation.

As the product has successfully completed a DCE, it can be used to downgrade the requirements of PROTECTED data in transit to those of UNCLASSIFIED, in accordance with the Australian Government Information Security Manual (ISM).

Enterprise-scale wireless networks typically comprise of three main elements:

- Supplicants: devices that support the 802.1X protocol, and are therefore able to authenticate to a wireless Access Point (AP) or Ethernet switch.
- Access Points: devices that relay data between the Supplicant and the RADIUS Server.
- RADIUS (Remote Authentication Dial-In User Service) Servers: back-end management servers used for authentication, authorisation and accounting purposes.

The security of any enterprise-scale wireless network is dependent on each of these elements and how they interact with each other.

Agencies using Juniper Odyssey as part of a wireless network MUST adhere to the following recommendations (1 through 14).

1. Juniper Odyssey MUST be used in conjunction with Access Points and RADIUS Servers that have successfully completed a DCE.
2. Supplicants take on the classification of the network they are connected to and MUST be treated as such.
3. The AP-to-RADIUS Server connection MUST be either:
   - Provided via a wired link that has been accredited to communicate classified data, or
   - Encapsulated with an additional layer of encryption (on top of the RADIUS encapsulation).

   If the second option is used, network encryption products (e.g. IPsec or SSL VPN products) that have successfully completed a DCE MUST be used to provide the additional layer of encryption.
4. Agencies MUST use WPA2 in Enterprise mode.
5. Agencies MUST use AES-CCMP for data confidentiality and integrity.
6. Mutual authentication MUST be performed via EAP-TLS with X.509 certificates for both Supplicant and RADIUS Server authentication.
7. Unique certificates MUST be used for both devices and users.
8. Agencies MUST use a PKI product or Hardware Security Module (HSM) that has completed a DCE to generate X.509 certificates.
9. Certificates used to grant access to a classified network take on the classification of the network and MUST be treated as such.
10. FIPS mode MUST be enabled on Juniper Odyssey.

11. Juniper Odyssey MUST be configured to validate the RADIUS Server's certificate.
12. Juniper Odyssey MUST NOT be configured to trust certificates generated by commercial certificate authorities.
13. Juniper Odyssey MUST be configured to only authenticate to trusted RADIUS Server names.
14. A trusted certificate chain MUST be stored on the Supplicant for the purposes of secure mutual authentication.

Recommendations given in this consumer guide take precedence over those in the ISM where there is a conflict.

Contact

For further information regarding the certification, cryptographic evaluation or compliance with the Information Security Manual please contact DSD on 1300 CYBER1 (1300 292 371) or email dsd.assist@defence.gov.au.

ISM 2012

The advice given in this document is in accordance with the Information Security Manual 2012. Australian government agencies are reminded to periodically check the latest release date of the ISM at http://www.dsd.gov.au/library/infosec/ism.html

Consumer Guide

This Consumer Guide was issued by DSD during May 2012.