Unified Threat Defence

This reference provides the necessary information to configure and manage Unified Threat Defence features within the network security architecture.

Unified threat defense

Unified Threat Defense (UTD) is Cisco's premier network security solution which provides a comprehensive suite of security features, such as:

- Enterprise Firewall
- Intrusion Prevention System (IPS)/Intrusion Detection System (IDS)
- Advanced Malware Protection
- URL Filtering, and
- DNS Security

Table 1: Feature History Table

Feature name	Release information	Feature description
Unified Threat Defense	Release 26.1.1	For enhanced protection across network, you can leverage Unified Threat Defense (UTD) which is Cisco's premier network security solution, to access a comprehensive suite of security features including: • Enterprise Firewall, IPS/IDS • Advanced Malware Protection • URL Filtering, and DNS Security

Unified threat defense restrictions

These product-specific restrictions apply.

- UTD container requires a minimum space of 1.8 GB.
- UTD is supported in both autonomous mode and controller mode, but in autonomous mode, only IPS/IDS features are supported.
- The UTD configuration supports the Cloud-Low profile only.
- On-Box Web-Filtering database is not supported.
- TLS decryption is not supported.

License requirements for UTD features

To enable UTD features, these licensing requirements apply:

- To enable UTD features in SD-Router (autonomous mode), you must have both a DNA Essentials license and a Network Essentials license.
- To use Cisco Secure Malware Analytics, you must have both a DNA Advantage license and a Network Advantage license.

References for unified threat defense configuration on IR8140

Configuration on the IR8140 is the same as on other products. For configuration information refer to:

- Unified Threat Defense Resource Profiles
- Intrusion Prevention System
- URL Filtering
- Advanced Malware Protection