



Support for DH group 5 Encryption under IKESA and IPSEC Transform Set

- [Feature Summary and Revision History, on page 1](#)
- [Feature Changes, on page 2](#)

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	<ul style="list-style-type: none"> • ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled – Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	<ul style="list-style-type: none"> • <i>ePDG Administration Guide</i>

Revision History

Revision Details	Release
ePDG supports Default DH group in non-trusted builds.	21.28.m7
ePDG supports Default DH group in trusted builds.	21.28.m5
First introduced.	21.17.12

Feature Changes

In earlier StarOS releases to be in compliant with network security, DH group 5 algorithm was identified as deprecated one and removed for trusted builds from 21.12.x onwards. In the StarOS 21.17.12 release, to support VoWiFi services for iPhone subscribers, ePDG supports DH group 5 algorithm for trusted builds and this DH group 5 algorithm can be configured under both IKESA and IPSEC transform set.

In the StarOS 21.28.5 and later releases, the default DH group for trusted builds in the **ikesa transform-set** is set as group 14. However, only in StarOS 21.28.5 and 21.28.m7 releases, the depreciated DH group 5 is available to configure as non-default configuration.