McAfee
Together is power.

DLP Endpoint
Migrating from 9.3 Environment

DLP Product Management

Migrating from DLPe 9.3 Environment

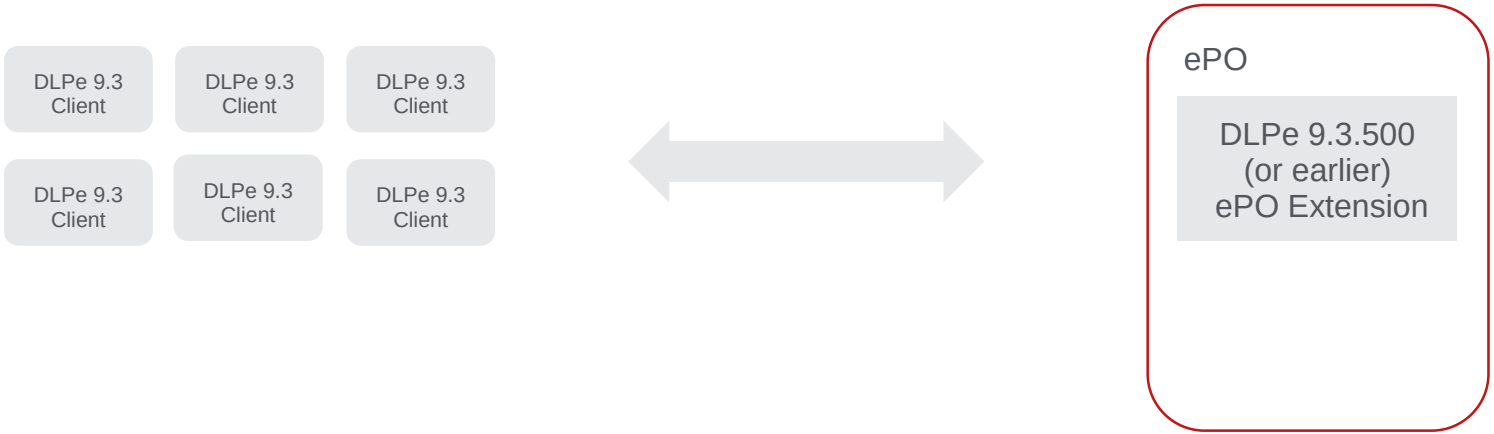
DLPe 9.4 onwards introduces a major enhancements to DLPe capabilities, in turn this implied policy and incident structure change. Hence the migration from 9.3 to later version requires a different procedure

This presentation provides guidance as for migrating a DLPe 9.3 environment to newer DLPe version 9.4/10.0/11.0
We do recommend to upgrade to latest release

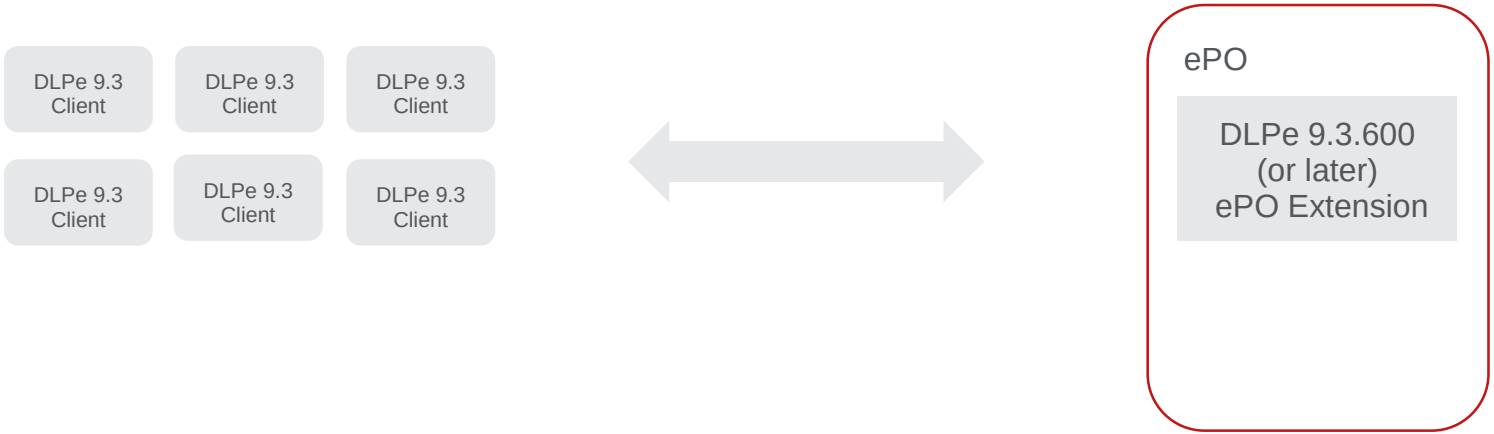
If your current environment is still prior to 9.3 (e.g. 9.2) , you need to upgrade to 9.3 first

The presentation uses 11.0 as an example but it is applicable to 9.4 and 10.0 as well

9.3 Environment – Starting point



Upgrade to 9.3.600 ePO extension (or later)



1. Only requires ePO extension upgrade
   No clients upgrade required

Install DLPe 11.0 ePO extension

DLPe 9.3 Client | DLPe 9.3 Client | DLPe 9.3 Client

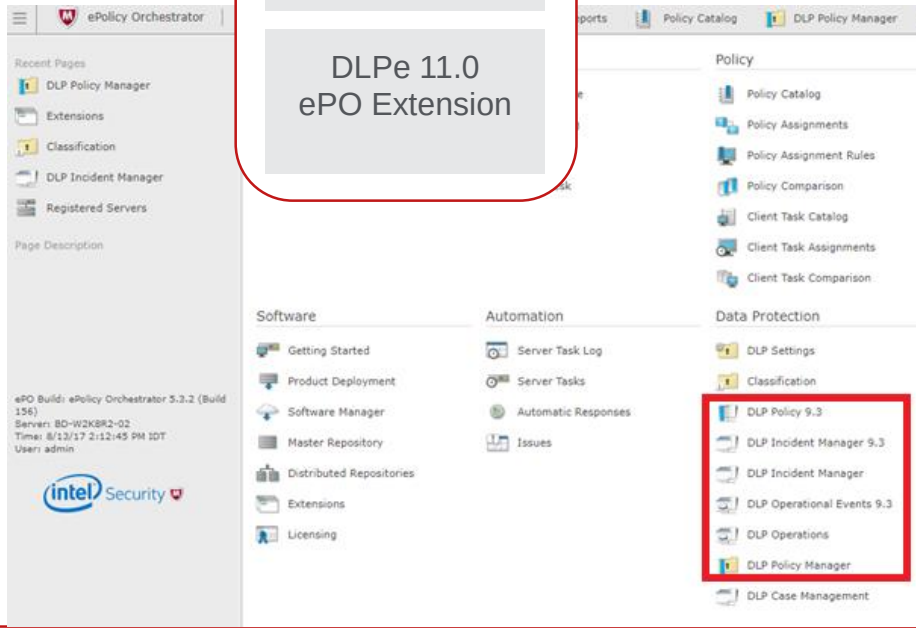
DLPe 9.3 Client | DLPe 9.3 Client | DLPe 9.3 Client

ePO

DLPe 9.3.600 (or later) ePO Extension

DLPe 11.0 ePO Extension

1. DLPe 11.0 is used as an example only , this is applicable to DLPe 9.4 ,10.0, and 11.0 (always deploy latest patches)
2. The DLPe 11.0 extension does NOT upgrade the 9.3.600 extension, both extensions run in parallel
3. Each extension manages its own clients
4. The 9.3 ePO modules (see screenshot) were renamed 9.3 (that's why we need 9.3.600 onwards)
5. At this stage DLPe 9.3 environment is fully operational, the DLPe 11.0 extension does not manage any client



Running Migration Tasks

DLPe 9.3 Client | DLPe 9.3 Client | DLPe 9.3 Client

DLPe 9.3 Client | DLPe 9.3 Client | DLPe 9.3 Client

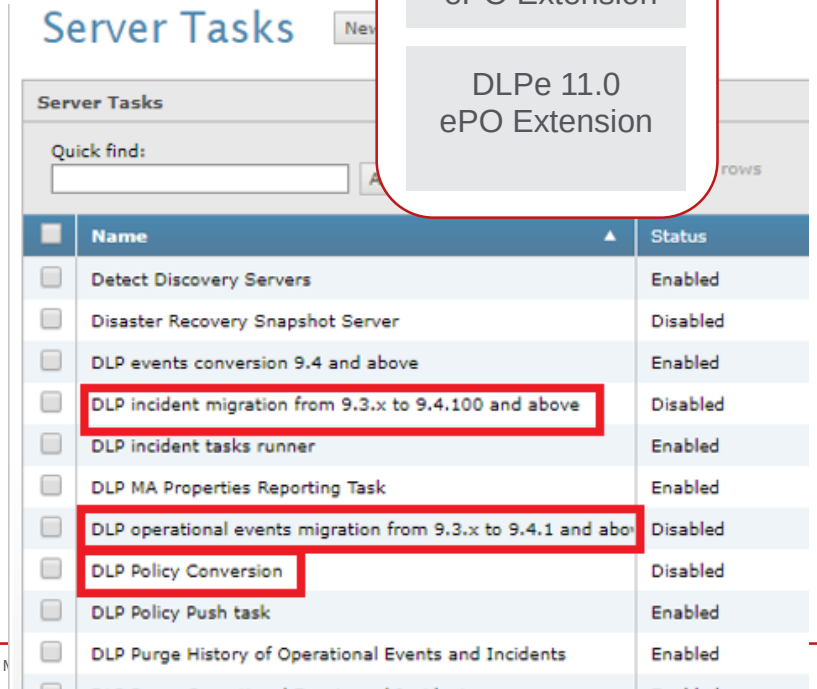
ePO

DLPe 9.3.600 (or later) ePO Extension

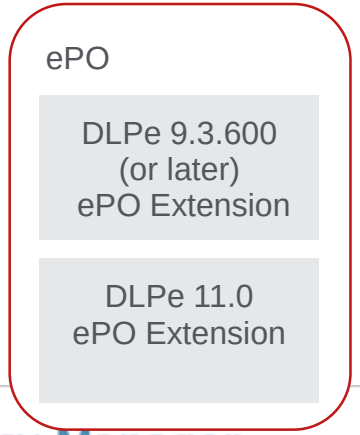
DLPe 11.0 ePO Extension

1. DLP 11.0 provides migration tasks for:
   - Policy
   - Incidents
   - Operational Events

2. At this stage, DLPe 9.3 environment is fully operational, the DLPe 11.0 extension does not manage any client



Policy Conversion task



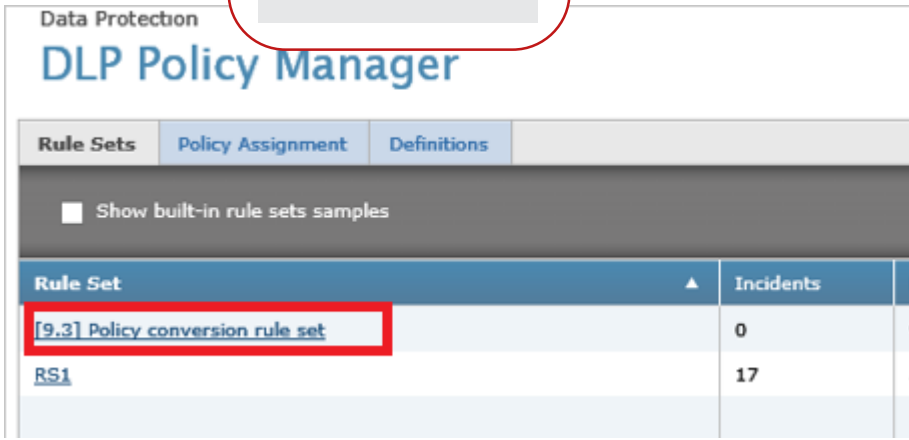
1. Converts the 9.3 Policy into a “9.3 ruleset” in the 11.0 ePO extension (single run), it is not part of a policy, and not yet applied

2. As 9.4 onwards offers multiple DLP polices, you may want to take use of the capability when creating polices in 9.4/10/11 environment

3. Conversion limitations are listed in KB85478

4. Main issue for conversion is for custom Regular Expression, DLPe 9.4 onwards uses RE2, which uses a different regex notation than the 9.3 Boost engine

5. At this stage, DLPe 9.3 environment is fully operational, the DLPe 11.0 extension does not manage any client



Incident Migration task

DLPe 9.3 Client | DLPe 9.3 Client | DLPe 9.3 Client

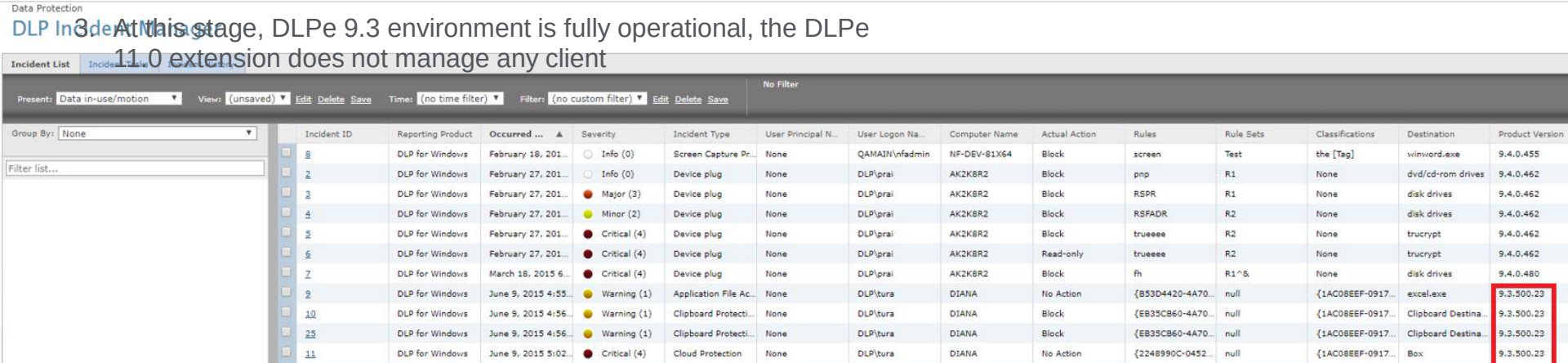
DLPe 9.3 Client | DLPe 9.3 Client | DLPe 9.3 Client

ePO

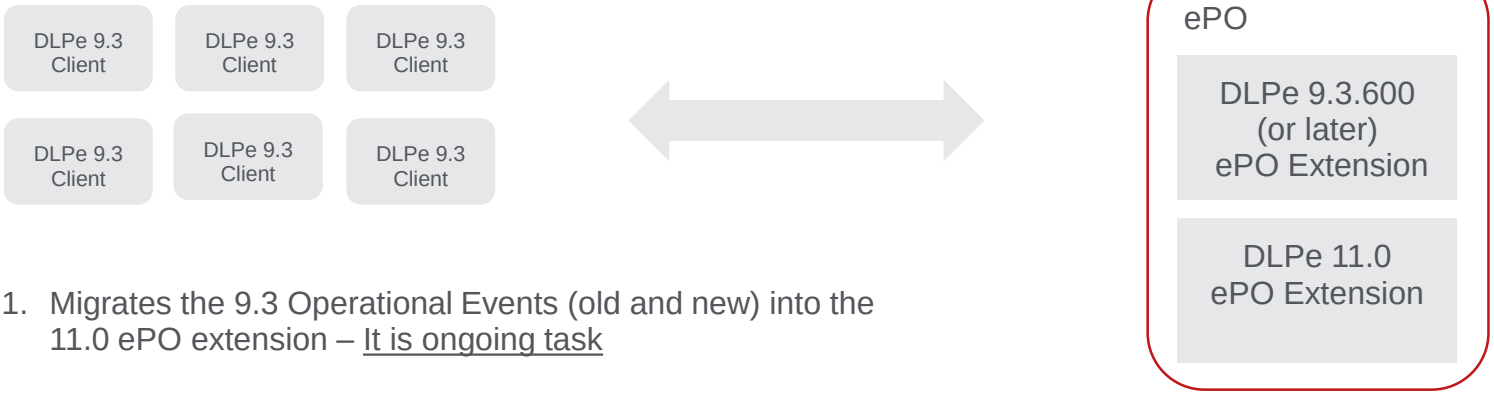
DLPe 9.3.600 (or later) ePO Extension

DLPe 11.0 ePO Extension

1. Migrates the 9.3 Incidents (old and new) into the 11.0 ePO extension – <u>It is ongoing task</u>
2. The 9.3 incidents are available both on the 9.3 extension and the 11.0 extension (see product version column)
3. At this stage, DLPe 9.3 environment is fully operational, the DLPe 11.0 extension does not manage any client



Operational Events Migration task

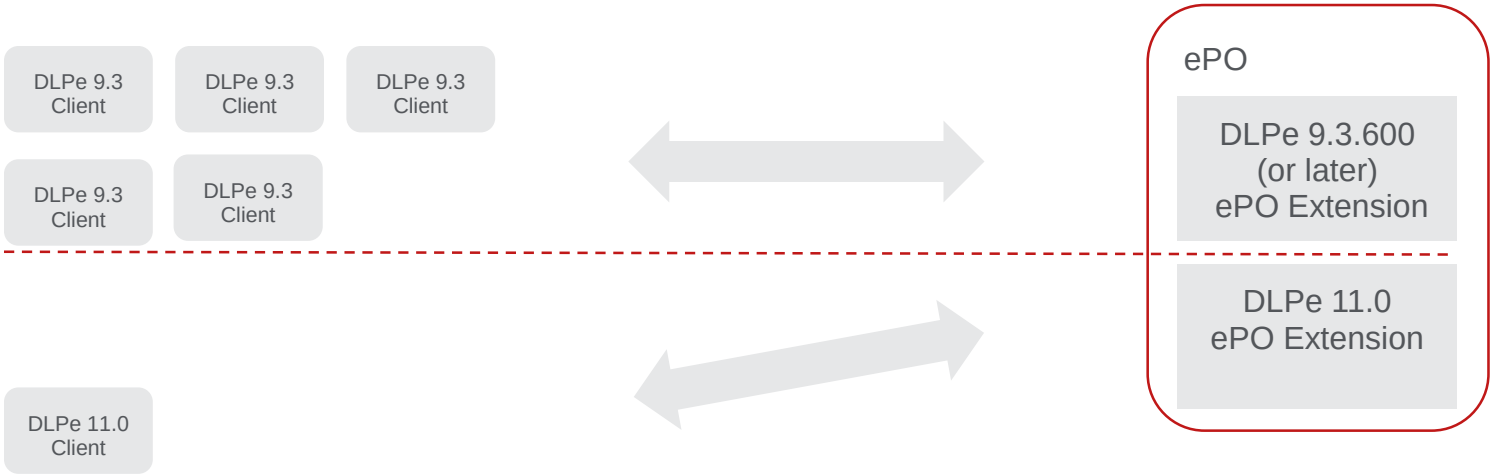


1. Migrates the 9.3 Operational Events (old and new) into the 11.0 ePO extension – It is ongoing task
2. The 9.3 Operational events are available both on the 9.3 extension and the 11.0 extension (see product version column)
3. At this stage, DLPe 9.3 environment is fully operational, the DLPe 11.0 extension does not manage any client

Migration status

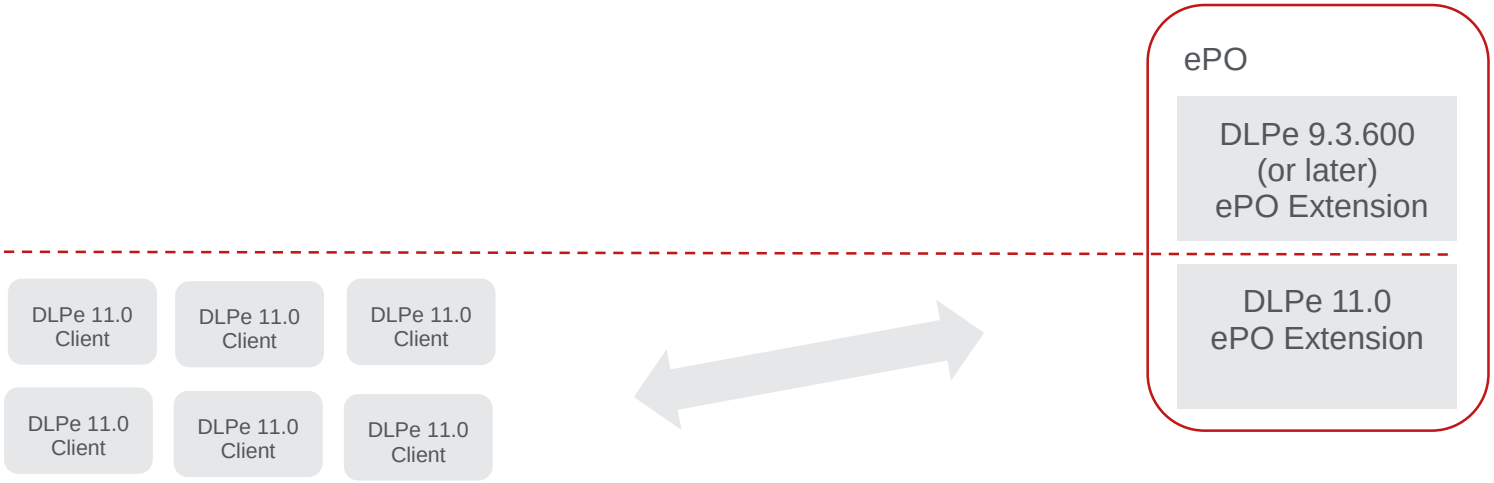
1. At this stage, DLPe 9.3 environment is fully operational, the DLPe 11.0 extension does not manage any client
2. DLPe 9.3 Policy converted to 11.0 structure, and ready to use
3. DLPe 9.3 incidents (old and new) are continuously migrated to the DLPe 11.0 environment. And available from both 9.3 and 11.0 extensions.
4. DLPe 9.3 Operational Events (old and new) are continuously migrated to the DLPe 11.0 environment. And available from both 9.3 and 11.0 extensions.

Start upgrading Clients



1. Start upgrading clients to 11.0
2. Upgraded clients automatically managed by the 11.0 ePO extension
3. DLPe 11.0 policy based on converted and adjusted 9.3 policy, or new policy
4. Incidents and operational events coming from both 9.3 and 11.0 are shown unified in DLPe 11.0

Complete upgrading Clients



1. All clients are upgraded 11.0
2. 9.3.600 extension can be removed
3. Fully operational 11.0 environment

Upgrade to 11.0 done

A Video illustrating the procedure
(using 9.3 to 9.4.100 as an example)
is available at:

https://www.youtube.com/watch?v=sc7eia_Si3o