



DLP Endpoint Migrating from 9.3 Environment

DLP Product Management

Migrating from DLPe 9.3 Environment

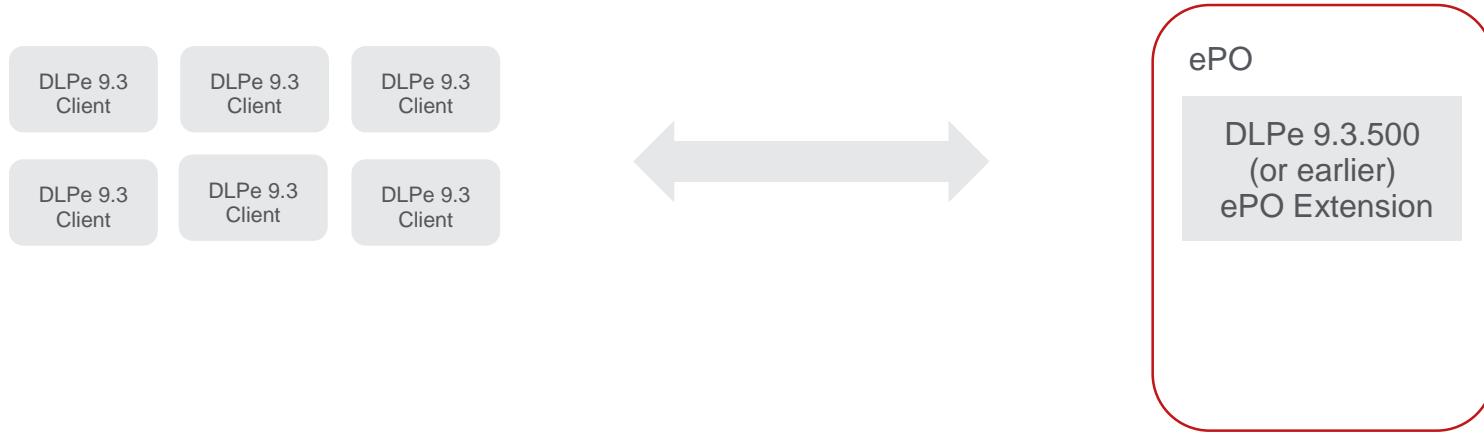
DLPe 9.4 onwards introduces a major enhancements to DLPe capabilities, in turn this implied policy and incident structure change. Hence the migration from 9.3 to later version requires a different procedure

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

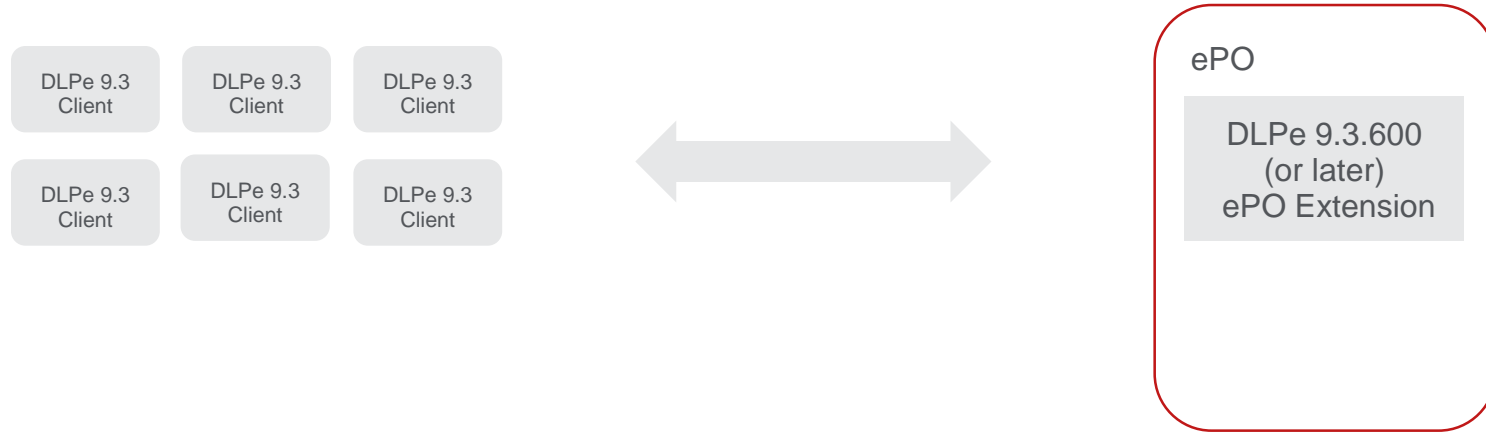
If your current environment is still prior to 9.3 (e.g. 9.2) , you need to upgrade to 9.3 first

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)

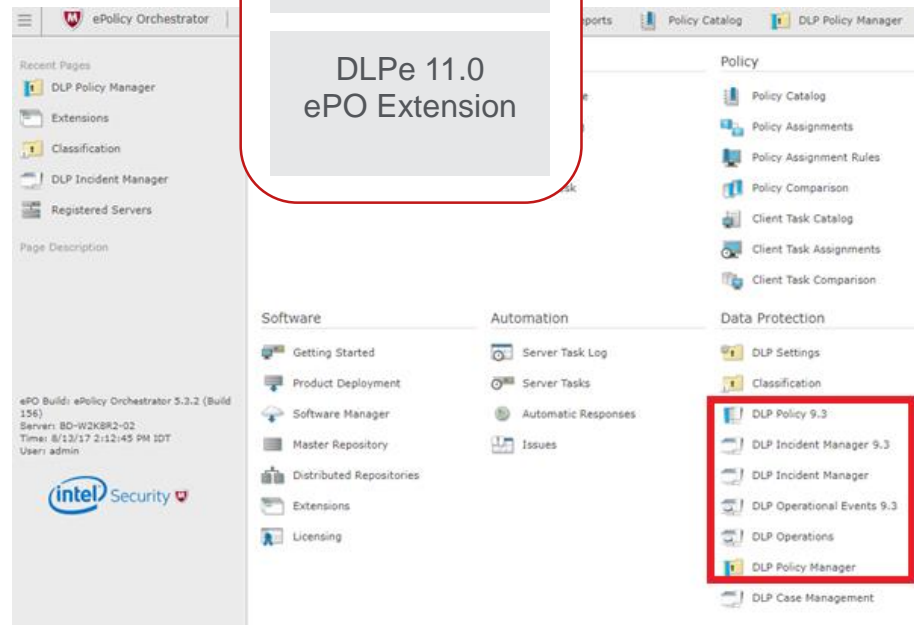
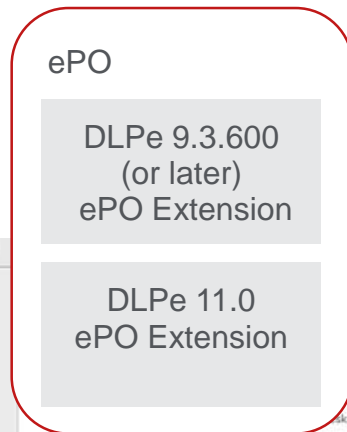


1. Only requires ePO extension upgrade
No clients upgrade required

Install DLPe 11.0 ePO extension



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



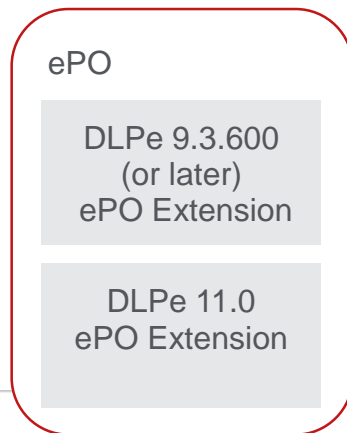
1. DLP 11.0 provides migration tasks for:
 - Policy
 - Incidents
 - Operational Events
2. At this stage, DLPe 9.3 environment is fully operational, the DLPe 11.0 extension does not manage any client

Server Tasks

Quick find:

<input type="checkbox"/>	Name	Status
<input type="checkbox"/>	Detect Discovery Servers	Enabled
<input type="checkbox"/>	Disaster Recovery Snapshot Server	Disabled
<input type="checkbox"/>	DLP events conversion 9.4 and above	Enabled
<input type="checkbox"/>	DLP incident migration from 9.3.x to 9.4.100 and above	Disabled
<input type="checkbox"/>	DLP incident tasks runner	Enabled
<input type="checkbox"/>	DLP MA Properties Reporting Task	Enabled
<input type="checkbox"/>	DLP operational events migration from 9.3.x to 9.4.1 and above	Disabled
<input type="checkbox"/>	DLP Policy Conversion	Disabled
<input type="checkbox"/>	DLP Policy Push task	Enabled
<input type="checkbox"/>	DLP Purge History of Operational Events and Incidents	Enabled

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

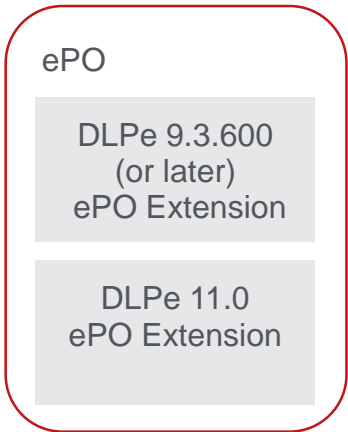
Data Protection
DLP Policy Manager

Rule Sets | Policy Assignment | Definitions

Show built-in rule sets samples

Rule Set	Incidents
[9.3] Policy conversion rule set	0
RS1	17

Incident Migration task



1. Migrates the 9.3 Incidents (old and new) into the 11.0 ePO extension – It is ongoing task
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

Incident ID	Reporting Product	Occurred ...	Severity	Incident Type	User Principal N...	User Logon Na...	Computer Name	Actual Action	Rules	Rule Sets	Classifications	Destination	Product Version
1	DLP for Windows	February 18, 201...	Info (0)	Screen Capture Pr...	None	QAMAIN\infadmin	NF-DEV-81X64	Block	screen	Test	the [Tag]	winword.exe	9.4.0.455
2	DLP for Windows	February 27, 201...	Info (0)	Device plug	None	DLP\prai	AK2KBR2	Block	pnp	R1	None	dvd/cd-rom drives	9.4.0.462
3	DLP for Windows	February 27, 201...	Major (3)	Device plug	None	DLP\prai	AK2KBR2	Block	RSPR	R1	None	disk drives	9.4.0.462
4	DLP for Windows	February 27, 201...	Minor (2)	Device plug	None	DLP\prai	AK2KBR2	Block	RSFADR	R2	None	disk drives	9.4.0.462
5	DLP for Windows	February 27, 201...	Critical (4)	Device plug	None	DLP\prai	AK2KBR2	Block	trueeee	R2	None	trcrypt	9.4.0.462
6	DLP for Windows	February 27, 201...	Critical (4)	Device plug	None	DLP\prai	AK2KBR2	Read-only	trueeee	R2	None	trcrypt	9.4.0.462
7	DLP for Windows	March 18, 2015 6...	Critical (4)	Device plug	None	DLP\prai	AK2KBR2	Block	fh	R1^&	None	disk drives	9.4.0.480
8	DLP for Windows	June 9, 2015 4:55...	Warning (1)	Application File Ac...	None	DLP\tura	DIANA	No Action	{B53D4420-4A70...	null	{1AC08EEF-0917...	excel.exe	9.3.500.23
10	DLP for Windows	June 9, 2015 4:56...	Warning (1)	Clipboard Protecti...	None	DLP\tura	DIANA	Block	{EB35C860-4A70...	null	{1AC08EEF-0917...	Clipboard Destina...	9.3.500.23
25	DLP for Windows	June 9, 2015 4:56...	Warning (1)	Clipboard Protecti...	None	DLP\tura	DIANA	Block	{EB35C860-4A70...	null	{1AC08EEF-0917...	Clipboard Destina...	9.3.500.23
11	DLP for Windows	June 9, 2015 5:02...	Critical (4)	Cloud Protection	None	DLP\tura	DIANA	No Action	{2248990C-0452...	null	{1AC08EEF-0917...	Box	9.3.500.23

Operational Events Migration task



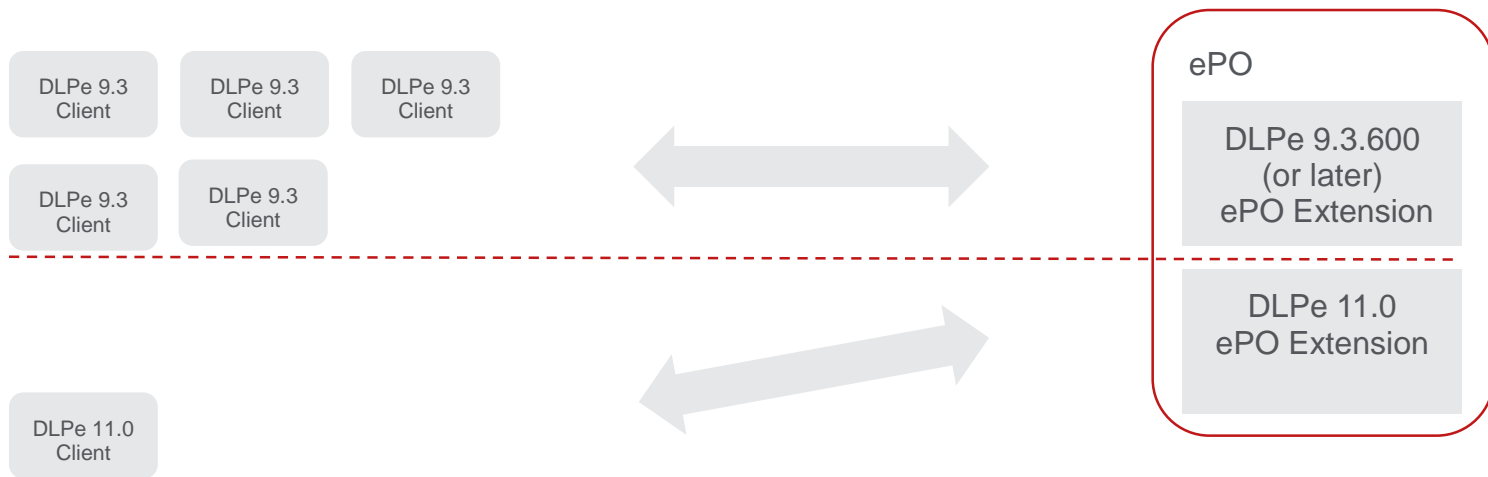
1. Migrates the 9.3 Operational Events (old and new) into the 11.0 ePO extension – It is ongoing task
2. The 9.3 Operational events are available both on the 9.3 extension and the 11.0 extension (see product version column)
3. At this stage, DLPe 9.3 environment is fully operational, the DLPe 11.0 extension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

Migration status



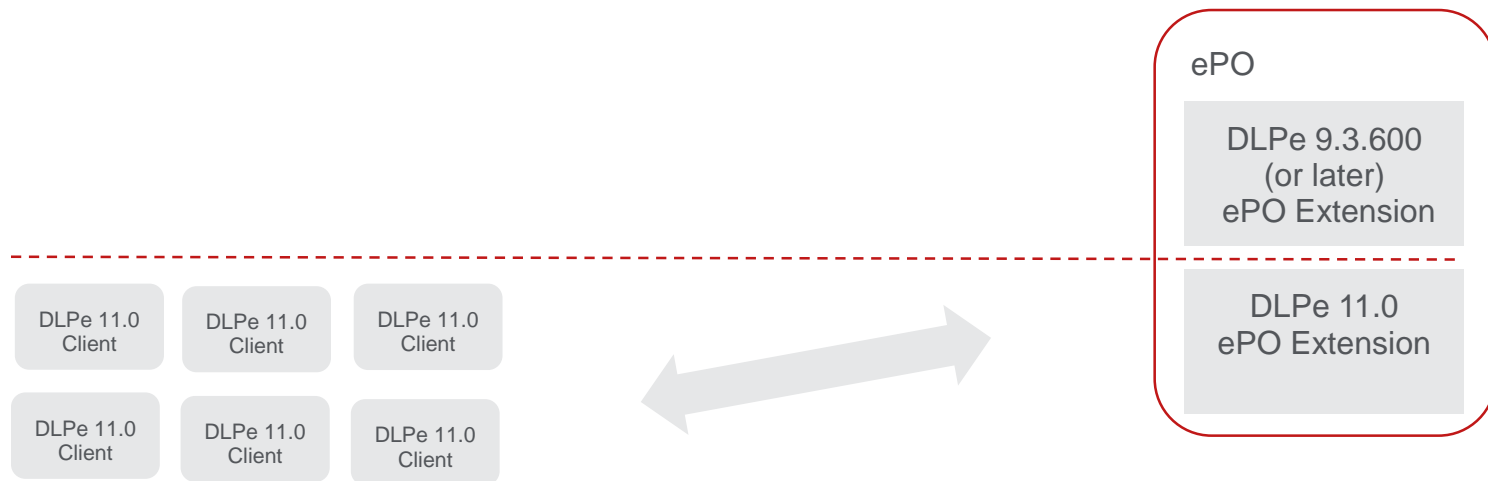
1. At this stage, DLPe 9.3 environment is fully operational, the DLPe 11.0 extension does not manage any client
2. DLPe 9.3 Policy converted to 11.0 structure, and ready to use
3. DLPe 9.3 incidents (old and new) are continuously migrated to the DLPe 11.0 environment. And available from both 9.3 and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



McAfee, the McAfee logo and [insert <other relevant McAfee Names>] are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the U.S. and/or other countries. Other names and brands may be claimed as the property of others. Copyright © 2017 McAfee LLC.