

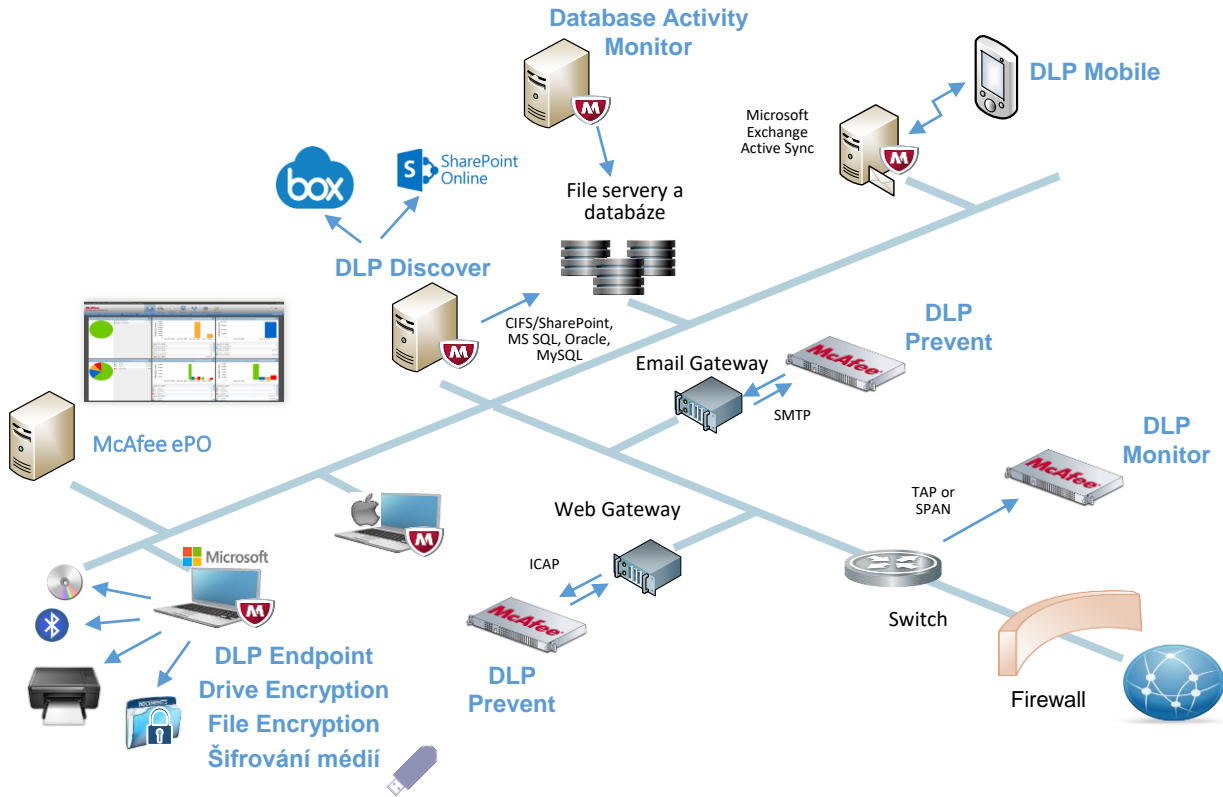


GDPR a ochrana dat produkty McAfee

Jan Strnad, Sales Engineer, McAfee

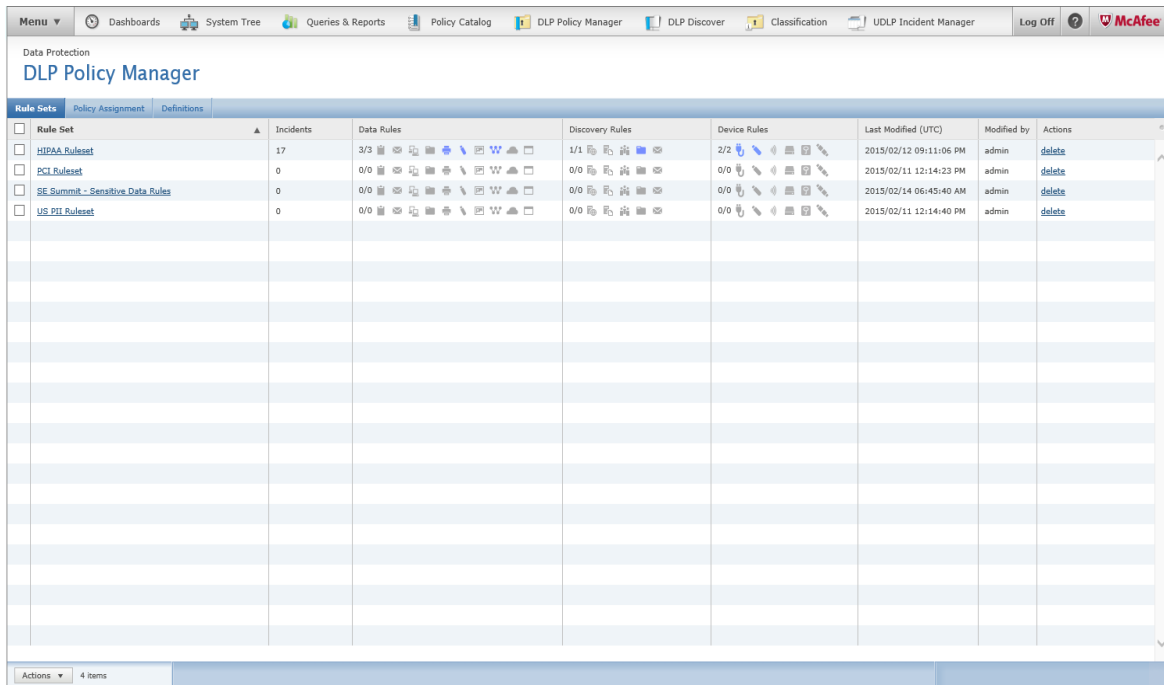


Komplexní ochrana dat s McAfee produkty



Jednotná politika pro Host i Network DLP

- DLP umožňuje definovat více rulesetů
- DLP rulesety je možné následně uplatňovat na různé skupiny počítačů
- DLP ruleset obsahuje pravidla Device Controlu, DLP a Discovery
- Flexibilní uplatnění různých rulesetů na různé skupiny počítačů a DLP systémů



The screenshot displays the McAfee DLP Policy Manager interface. At the top, there is a navigation menu with options like Dashboards, System Tree, Queries & Reports, Policy Catalog, DLP Policy Manager, DLP Discover, Classification, and UIDLP Incident Manager. The main title is "Data Protection DLP Policy Manager". Below this, there are tabs for "Rule Sets", "Policy Assignment", and "Definitions". The "Rule Sets" tab is active, showing a table with the following columns: Rule Set, Incidents, Data Rules, Discovery Rules, Device Rules, Last Modified (UTC), Modified by, and Actions.

Rule Set	Incidents	Data Rules	Discovery Rules	Device Rules	Last Modified (UTC)	Modified by	Actions
<input type="checkbox"/> HIPAA Ruleset	17	3/3	1/1	2/2	2015/02/12 09:11:06 PM	admin	delete
<input type="checkbox"/> PCI Ruleset	0	0/0	0/0	0/0	2015/02/11 12:14:23 PM	admin	delete
<input type="checkbox"/> SE Summit - Sensitive Data Rules	0	0/0	0/0	0/0	2015/02/14 06:45:40 AM	admin	delete
<input type="checkbox"/> US PII Ruleset	0	0/0	0/0	0/0	2015/02/11 12:14:40 PM	admin	delete

At the bottom left, there is an "Actions" dropdown menu showing "4 items".

DLP rulesety – DLP politika

- Seznam pravidiel DLP systému v rulesetu
- Definice DLP pravidla - podmínky pro Email protection pravidlo
- Definice DLP pravidla – reakce pro Email protection pravidlo

DLP Policy Manager


DLP Rule Set										
Name:		Demo ruleset					Save			
Note:										
Data Protection										
Device Control										
Discovery										
	State	Rule	Severity	Incidents	Data To Protect	Applies To	Protection	Enforce On	Endpoint Online	E
<input type="checkbox"/>		Clipboard - Block Rodne cisla	Critical	0	Rodne cislo RegEx	any user	Clipboard Protection		Block	S
<input type="checkbox"/>		Cloud - block Credit cards	Major	0	Credit cards RegEx	any user	Cloud Protection		Block	S
<input type="checkbox"/>		Email - Block Credit cards	Major	13	Credit cards RegEx	any user	Email Protection		Block	S
<input type="checkbox"/>		Email - Block Finance data	Critical	31	Finance data share	any user	Email Protection		Block	S
<input type="checkbox"/>		Email - Justification Rodna cisla	Critical	27	Rodne cislo RegEx	any user	Email Protection		Request justifica	S
<input type="checkbox"/>		Email - Monitor PPT data	Major	2	PowerPoint data creation	any user	Email Protection		No Action	S
<input type="checkbox"/>		Reputation - Block sensitive data with TIE reputation unkn	Major	27	Credit cards RegEx,Finance data s	any user	Application File Access Protect		Block	S
<input type="checkbox"/>		USB - Block Credit cards	Major	9	Credit cards RegEx	any user	Removable Storage Protection		Block	S
<input type="checkbox"/>		USB - Justification Rodna cisla	Major	3	Rodne cislo RegEx	any user	Removable Storage Protection		Request justifica	S
<input type="checkbox"/>		USB - Block Finance data	Critical	1	Finance data share	any user	Removable Storage Protection		Block	S
<input type="checkbox"/>		USB - Encrypt Sensitive data	Major	12	Sensitive manual tag	any user	Removable Storage Protection		Encrypt	S
<input type="checkbox"/>		USB - Monitor all non sensitive data	Warning	5	Not Classified	any user	Removable Storage Protection		No Action	S

DLP rulesety – DLP politika

- Seznam pravidel DLP systému v rulesetu
- Definice DLP pravidla - podmínky pro Email protection pravidlo
- Definice DLP pravidla – reakce pro Email protection pravidlo

DLP Policy Manager

DLP Rule Set - Demo ruleset

 **Email Protection**

Rule Name:

State: Enabled Disabled Severity: Critical Low

Enforce On: McAfee DLP Endpoint for Windows McAfee DLP Prevent

Condition Exceptions Reaction

Classification of

(*) if there are multiple conditions of type "one of the attachments", they are all evaluated for the same attachment file

and **Sender**

and **Email Envelope**


and **Recipient** List includes

DLP rulesety – DLP politika

- Seznam pravidel DLP systému v rulesetu
- Definice DLP pravidla - podmínky pro Email protection pravidlo
- Definice DLP pravidla – reakce pro Email protection pravidlo

DLP Policy Manager

DLP Rule Set - Demo ruleset

 **Email Protection**

Rule Name:

State: Disabled Enabled Severity: Low Critical High

Enforce On: McAfee DLP Endpoint for Windows McAfee DLP Prevent

Condition **Exceptions** **Reaction**

McAfee DLP Endpoint

Computer connected to corporate network

Action:

User Notification: ...

Report Incident: Report Incident
 Store original email as evidence

Computer disconnected from the corporate network

Action:

McAfee DLP Prevent

Action:

Report Incident: Report Incident Store original email as evidence

DLP Incident Manager

- Incident Manager zobrazuje detekované události z :
 - DLP Endpoint – Data in-use/motion
 - DLP Local discovery – Data at rest – endpoint
 - DLP Network discovery – Data at rest - network

The screenshot displays the McAfee ePolicy Orchestrator (ePO) interface, specifically the DLP Incident Manager section. The interface is titled "Data Protection DLP Incident Manager" and shows a list of incidents under the "Incident List" tab. The "Present:" dropdown is set to "Data in-use/motion". The table below lists various incidents with columns for Incident ID, Reporting P..., Occur..., Severity, Incident Type, User Princip..., User Logon..., Computer N..., Actual Action, Rules, Rule Sets, Classificati..., and Destination.

Incident ID	Reporting P...	Occur...	Severity	Incident Type	User Princip...	User Logon...	Computer N...	Actual Action	Rules	Rule Sets	Classificati...	Destination
156	DLP for Winds...	January 19, 2...	Major (3)	Email Protect...	Administrator...	DEMO\Admini...	WS_WIN7_2	Block	Email - Block...	Demo ruleset	Credit cards R...	tiscali.cz
155	DLP for Winds...	January 19, 2...	Major (3)	Email Protect...	Administrator...	DEMO\Admini...	WS_WIN7_2	Block	Email - Block...	Demo ruleset	Credit cards R...	tiscali.cz
154	DLP for Winds...	January 19, 2...	Major (3)	Email Protect...	Administrator...	DEMO\Admini...	WS_WIN7_2	Block	Email - Block...	Demo ruleset	Credit cards R...	tiscali.cz
153	DLP for Winds...	January 19, 2...	Critical (4)	Email Protect...	Administrator...	DEMO\Admini...	WS_WIN7_2	Block	Email - Justif...	Demo ruleset	Rodne cislo R...	tiscali.cz
152	DLP for Winds...	January 19, 2...	Critical (4)	Device plug	Administrator...	DEMO\Admini...	WS_WIN7_2	Block	Block Kingsto...	Demo ruleset	None	disk drives
151	DLP for Winds...	January 19, 2...	Major (3)	Device plug	Administrator...	DEMO\Admini...	WS_WIN7_2	Block	File access bl...	Demo ruleset	None	disk drives
150	DLP for Winds...	January 17, 2...	Critical (4)	Email Protect...	Administrator...	DEMO\Admini...	WS_WIN7	Block	Email - Block...	Demo ruleset	Finance data ...	tiscali.cz
149	DLP for Winds...	January 11, 2...	Major (3)	Email Protect...	Administrator...	DEMO\Admini...	WS_WIN7	No Action	Email - Monit...	Demo ruleset	PowerPoint d...	tiscali.cz
148	DLP for Winds...	January 11, 2...	Critical (4)	Email Protect...	Administrator...	DEMO\Admini...	WS_WIN7	Block	Email - Justif...	Demo ruleset	Rodne cislo (1)	tiscali.cz
147	DLP for Winds...	January 6, 20...	Major (3)	Removable St...	Administrator...	DEMO\Admini...	WS_WIN7	Block	USB - Block C...	Demo ruleset	Credit cards (...)	Disk drives
146	DLP for Winds...	January 6, 20...	Major (3)	Removable St...	Administrator...	DEMO\Admini...	WS_WIN7	No Action	USB - Justific...	Demo ruleset	Rodne cislo (2)	Disk drives
145	DLP for Winds...	January 6, 20...	Major (3)	Removable St...	Administrator...	DEMO\Admini...	WS_WIN7	Encrypt	USB - Encrypt...	Demo ruleset	Sensitive	Disk drives
144	DLP for Winds...	January 6, 20...	Warning	Removable St...	Administrator...	DEMO\Admini...	WS_WIN7	No Action	USB - Monitor...	Demo ruleset	NOT CLASSIF...	Disk drives
143	DLP for Winds...	January 6, 20...	Major (3)	Device plug	Administrator...	DEMO\Admini...	WS_WIN7	Block	File access bl...	Demo ruleset	None	disk drives
142	DLP for Winds...	January 6, 20...	Major (3)	Device plug	Administrator...	DEMO\Admini...	WS_WIN7	Read-only	File access bl...	Demo ruleset	None	disk drives
141	DLP for Winds...	January 6, 20...	Critical (4)	Device plug	Administrator...	DEMO\Admini...	WS_WIN7	Block	Block Kingsto...	Demo ruleset	None	disk drives
140	DLP for Winds...	January 6, 20...	Major (3)	Device plug	Administrator...	DEMO\Admini...	WS_WIN7	Read-only	Read-Only Co...	Demo ruleset	None	disk drives
139	DLP for Winds...	January 6, 20...	Minor (2)	Device plug	Administrator...	DEMO\Admini...	WS_WIN7	No Action	Monitor Patri...	Demo ruleset	None	disk drives
138	DLP for Winds...	January 6, 20...	Major (3)	Removable St...	Administrator...	DEMO\Admini...	WS_WIN7	Block	USB - Justific...	Demo ruleset	Rodne cislo (2)	Disk drives
137	DLP for Winds...	January 6, 20...	Minor (2)	Device plug	Administrator...	DEMO\Admini...	WS_WIN7	No Action	Monitor Patri...	Demo ruleset	None	disk drives
136	DLP for Winds...	January 6, 20...	Major (3)	Device plug	Administrator...	DEMO\Admini...	WS_WIN7	Read-only	Read-Only Co...	Demo ruleset	None	disk drives
135	DLP for Winds...	January 6, 20...	Minor (2)	Device plug	Administrator...	DEMO\Admini...	WS_WIN7	No Action	Monitor Patri...	Demo ruleset	None	disk drives
134	DLP for Winds...	January 6, 20...	Major (3)	Removable St...	Administrator...	DEMO\Admini...	WS_WIN7	Encrypt	USB - Encrypt...	Demo ruleset	Sensitive	Disk drives
133	DLP for Winds...	January 6, 20...	Major (3)	Removable St...	Administrator...	DEMO\Admini...	WS_WIN7	Block	USB - Block C...	Demo ruleset	Credit cards (...)	Disk drives

DLP Incident Manager – detail událostí

- Kliknutím na událost se zobrazuje kompletní detail události
 - Počítač, IP adresa, uživatel, aplikace, DLP politika.....
 - Datum a čas, provedená akce, typ incidentu, pravidlo.....
 - Další detaily – email, typ zařízení

The screenshot displays the McAfee ePolicy Orchestrator interface, specifically the DLP Incident Manager section. The incident details are as follows:

Section	Field	Value
General Details	Incident ID:	156
	Occurred (UTC):	January 19, 2017 3:44:03 PM
	Occurred (Endpoint):	January 19, 2017 3:44:03 PM Coordinated Universal Time
	Incident Type:	Email Protection
	Actual Action:	Block
	Expected Action:	Block
	Severity:	Major
	Status:	New
	Resolution:	None
	Reviewer:	Unassigned
Labels:		
Source	Computer Name:	WS_WIN7_2
	Computer IP:	192.168.1.110
	User Principal Name (username@fqdn):	Administrator@demo.local
	Connectivity State:	Online
	Product Version:	10.0.100.37
	Policy Name:	My Default DLP Policy (28)
Source Application:	outlook.exe	
Reporting Product:	DLP for Windows	
Destination	Sender:	jan_strnad@fiscall.cz
	To:	jan_strnad@fiscall.cz
	Email Subject:	credit cards numbers.xlsx
	Matched Recipients:	jan_strnad@fiscall.cz
All Recipients:	jan_strnad@fiscall.cz	

Evidence Name	File Size (KB)	Match Count	Short Match String	Classifications	Path
credit_cards_numbers.xlsx.msg	28	5			
credit_cards_numbers.xlsx	1	0			
credit_cards_numbers.xlsx	7	5	Firma 1 1234-1742-1478-2586 Firma 2 1584-1457-2178-273	Credit cards RegEx (5)	



McAfee, the McAfee logo and 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.