

Managing Forefront Endpoint Protection with System Center Configuration Manager

Stefan Schörling – Schörling & Co AB

stefan@msfaq.se



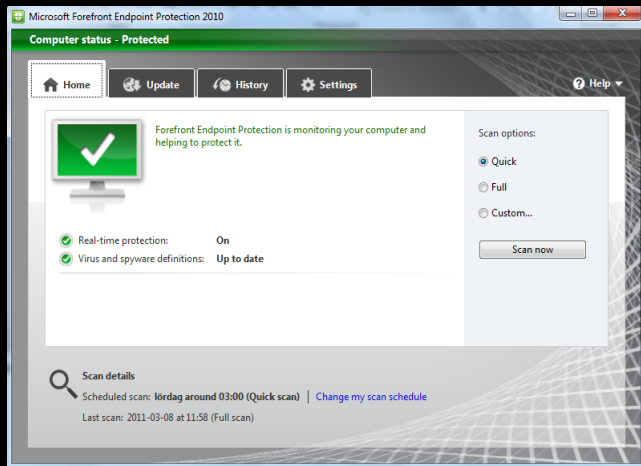
Agenda

- FEP 2010 Bakgrund & Överblick
- Vad FEP ger för skydd
- FEP Arkitektur
- FEP Installation & Hantering

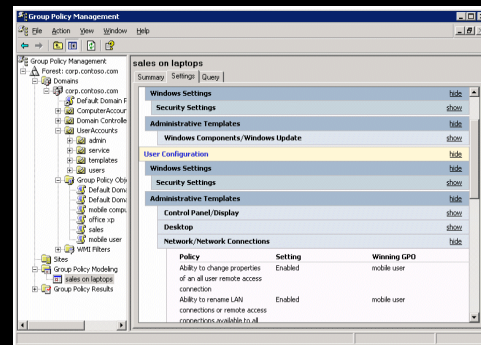


FEP 2010 - Managerbarhet

Standalone



+ GPO



+ Operations Manager

Endpoints with FEP

Look for: Find Now Clear

State	N...	Antimalware Engine	Antimalware Activity	Antimalware Definitions	Last Quick Scan End (GMT)	Client Version
Healthy	S...	Healthy	Healthy	Healthy	2011-02-05 00:06:47	2.0.657.0
Healthy	s...	Healthy	Healthy	Healthy		2.0.657.0

FEP 2010 - Managerbarhet

The image displays two overlapping windows from the Microsoft Forefront Endpoint Protection 2010 suite. The left window, titled 'Microsoft Forefront Endpoint Protection 2010', shows the 'Computer status - Protected' view. It features a green checkmark icon and text stating 'Forefront Endpoint Protection is monitoring your computer and helping to protect it.' Below this, there are scan options: 'Quick' (selected), 'Full', and 'Custom...'. A 'Scan now' button is also present. The status section shows 'Real-time protection: On' and 'Virus and spyware definitions: Up to date'. At the bottom, 'Scan details' indicate a scheduled scan for 'lördag around 03:00 (Quick scan)' and a last scan on '2011-03-08 at 11:58 (Full scan)'. The right window, titled 'Configuration Manager Console', shows a tree view on the left with 'Forefront Endpoint Protection' selected. The main pane displays 'Forefront Endpoint Protection' dashboard information, including a 'Dashboard - Updated: 2011-03-17 17:18' and 'Operational Statistics'. A pie chart shows '100.0%' deployment. Below the chart is a legend for deployment status: 'Remo...' (0), 'Failed' (0), 'Pendi...' (0), 'Out o...' (0), and 'Deplo...' (311). Two tables provide further statistics: 'Client Deployment Status' and 'Security Status'. The 'Client Deployment Status' table shows 'Targeted by FEP: 311 out of 464'. The 'Security Status' table shows 'Infected' (0), 'Restart required' (0), 'Full scan required' (0), and 'Recent malware activity (last 2...)' (1). A third table, 'Definition Status', shows 'Older than 1 week' (16), 'Up to 7 days old' (31), 'Up to 3 days old' (146), and 'Up to date' (116). A fourth table, 'Protection Status', shows 'Protection service off' (0), 'Not reporting' (12), and 'Healthy' (299). A fifth table, 'Policy Distribution Status', shows 'Failed' (0), 'Pending' (17), and 'Distributed' (292). At the bottom, 'Forefront Endpoint Protection Baselines' are listed.

+ Configuration Manager

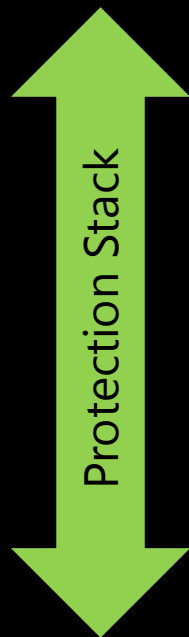
Client Deployment Status	Security Status	Computers
Targeted by FEP: 311 out of 464	Infected	0
	Restart required	0
	Full scan required	0
	Recent malware activity (last 2...)	1

Definition Status	Computers
Older than 1 week	16
Up to 7 days old	31
Up to 3 days old	146
Up to date	116

Protection Status	Computers
Protection service off	0
Not reporting	12
Healthy	299

Policy Distribution Status	Computers
Failed	0
Pending	17
Distributed	292

Skydd



Firewall & Configuration Management

Antimalware

Dynamic
Signature
Service

Generics and Heuristics

Behavior Monitoring

Browser Protection

Network Vulnerability Shielding

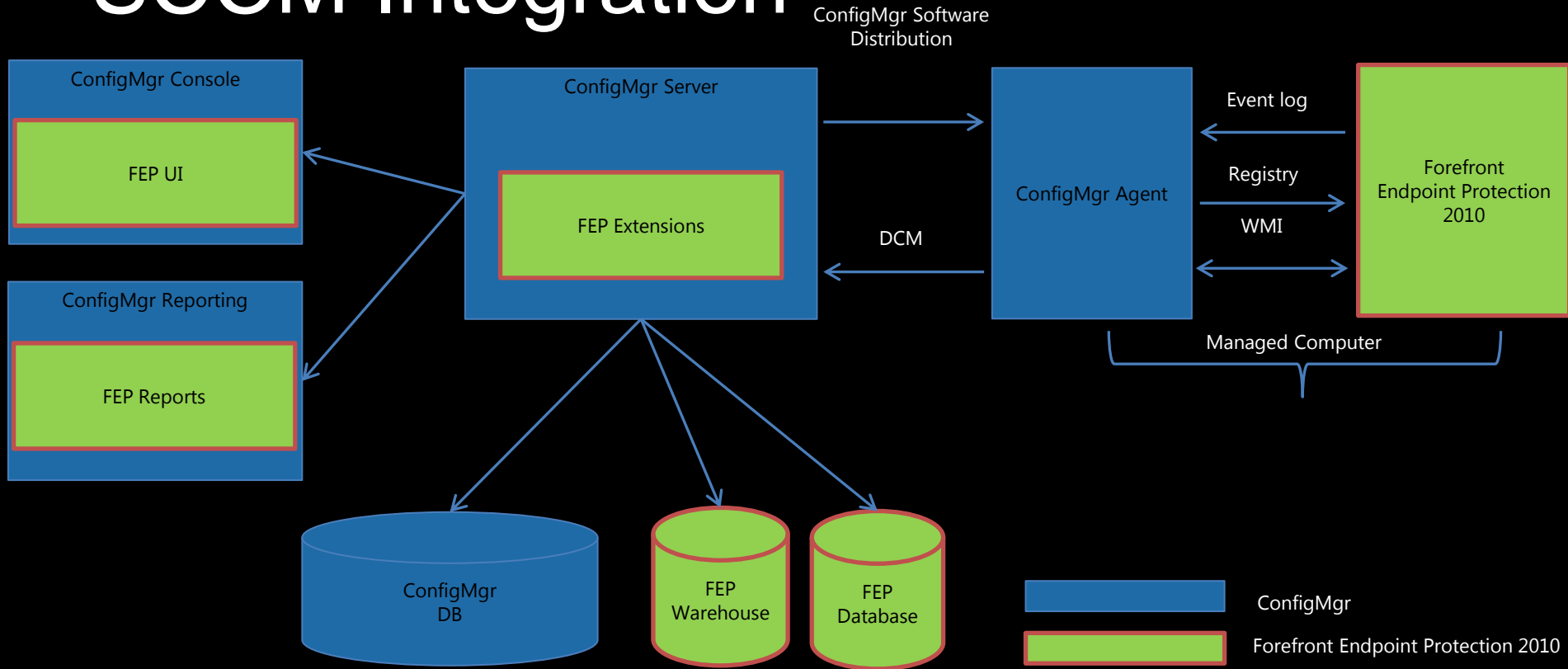
Anti-rootkit

Malware Response "MMPC"

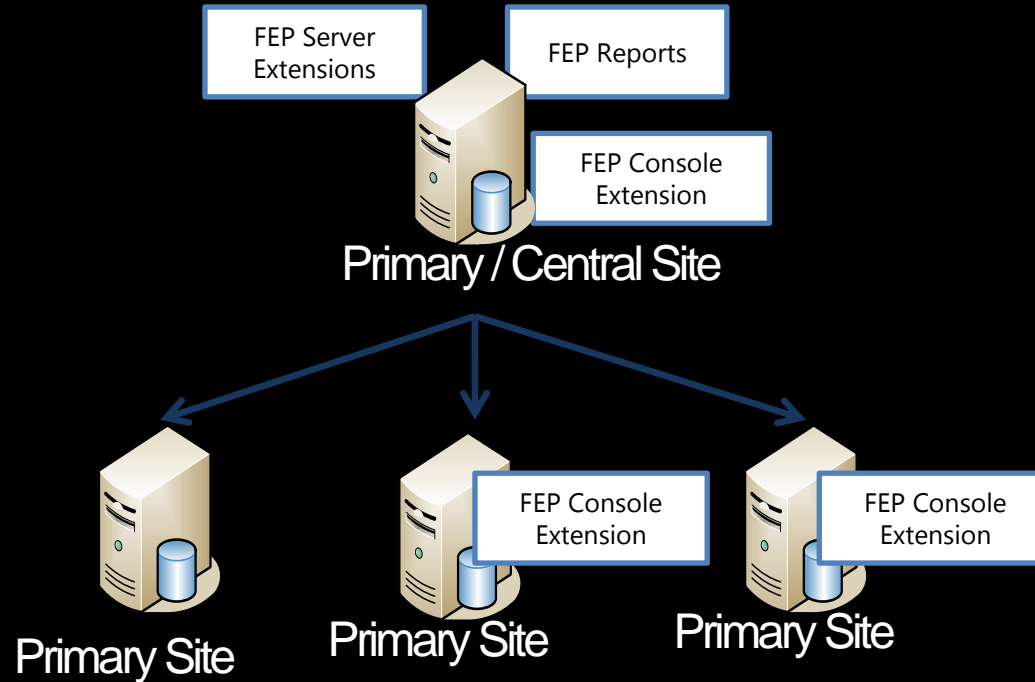
Skydd

Demo...

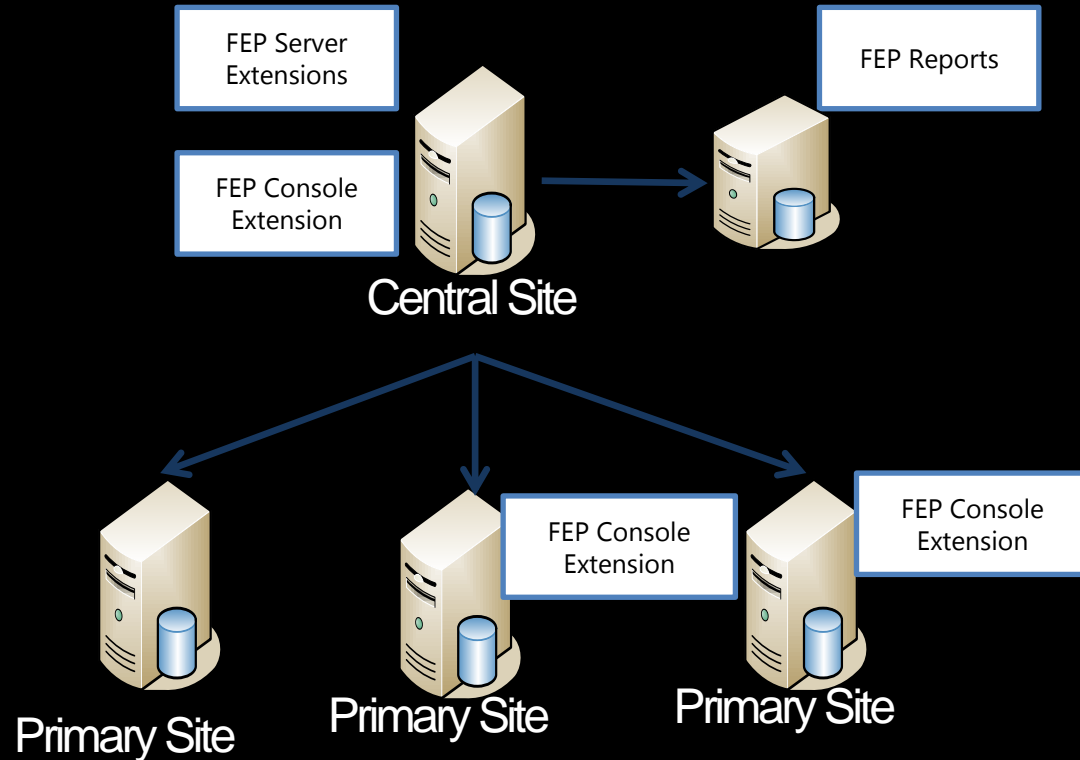
SCCM Integration



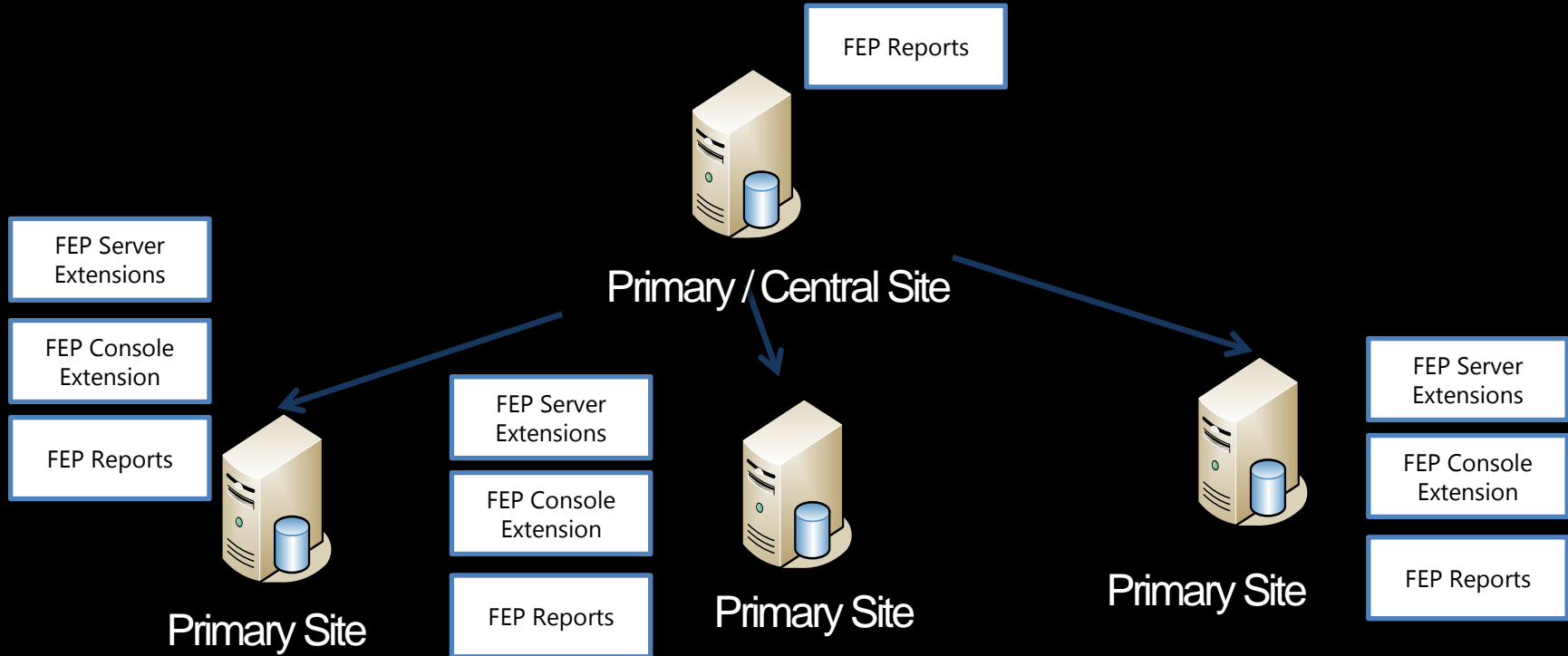
Basic



Basic + Remote Reporting



Advanced Installation



Planering

- Datawarehouse
- Exkluderingar
- Definitioner
 - Full ~55 MB
 - Delta ~
 - Binary Delta ~

Installation

Demo...

Upprensning

```
1 # This script removes files older than 30 days in the specified path
2
3 $logFolder = Get-ChildItem -path "D:\IISLogfiles" -include "*.log" -recurse
4 foreach($file in $logFolder)
5 {
6     $numberOfDaysOld = ((Get-Date) - $file.LastWriteTime).Days
7     if ($numberOfDaysOld -gt 30 -and $file.PsIsContainer -ne $True)
8     {
9         $file.Delete()
10    }
11 }
```

```
1 # This script cleans wsus from Superseded, Expired Updates and cleans the content
2 [reflection.assembly]::LoadWithPartialName("Microsoft.UpdateServices.Administration")
3 | out-null
4 $wsus = [Microsoft.UpdateServices.Administration.AdminProxy]::GetUpdateServer();
5 $cleanupScope = new-object Microsoft.UpdateServices.Administration.CleanupScope;
6 $cleanupScope.DeclineSupersededUpdates = $true
7 $cleanupScope.DeclineExpiredUpdates = $true
8 $cleanupScope.CleanupObsoleteUpdates = $true
9 $cleanupScope.CompressUpdates = $true
10 $cleanupScope.CleanupObsoleteComputers = $false
11 $cleanupScope.CleanupUnneededContentFiles = $true
12 $cleanupManager = $wsus.GetCleanupManager();
13 $cleanupManager.PerformCleanup($cleanupScope);
```

Inställningar och Larm

Demo...

From: fep-alerts@someonehackedmy.network [mailto:fep-alerts@someonehackedmy.network]

Sent: den 20 februari 2011 08:46

To: Stefan Schörling

Subject: Forefront Endpoint Protection Alert: Malware Detection



Forefront Endpoint Protection has detected malware on a computer in your organization.

Detection time (UTC): 2011-02-20 07:36:20

Computer name: STESCH,someonehackedmy.network

Malware name: Trojan:Win32/Tibs.IT

To view more information about malware activity in your organization, run a Computer List Report.

Note: No additional Malware Detection alerts will be generated for this computer for the next 24 hours.

Utrullning av klienter och
daglig hantering

Demo...

Rapportering

Demo...

Utmaningar

- Definitions Distribution
- Larmhantering
- FCS till FEP utan Config Mgr vana
- Tamper Protection
- SEP Live update not uninstalled

System Center User Group

www.scug.se

Live Groups

Facebook

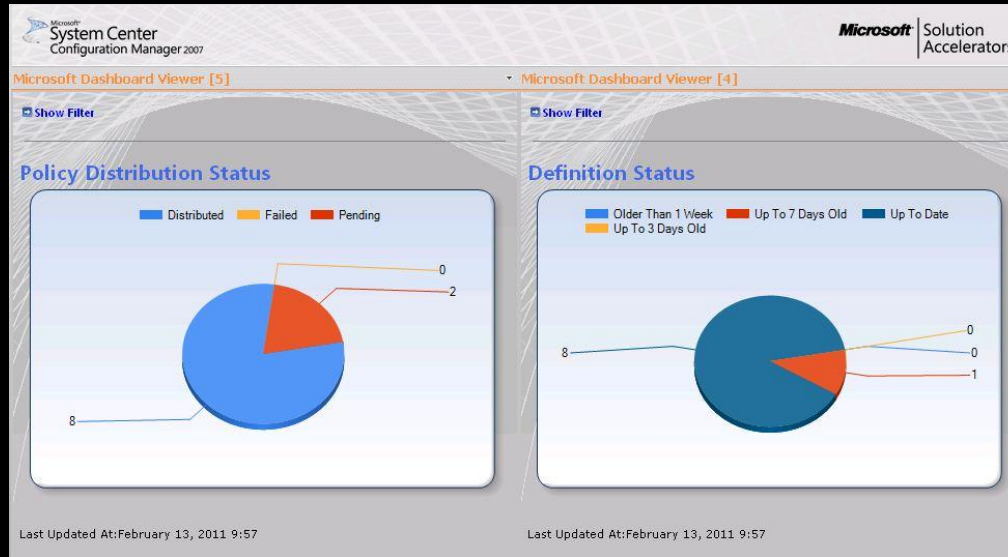


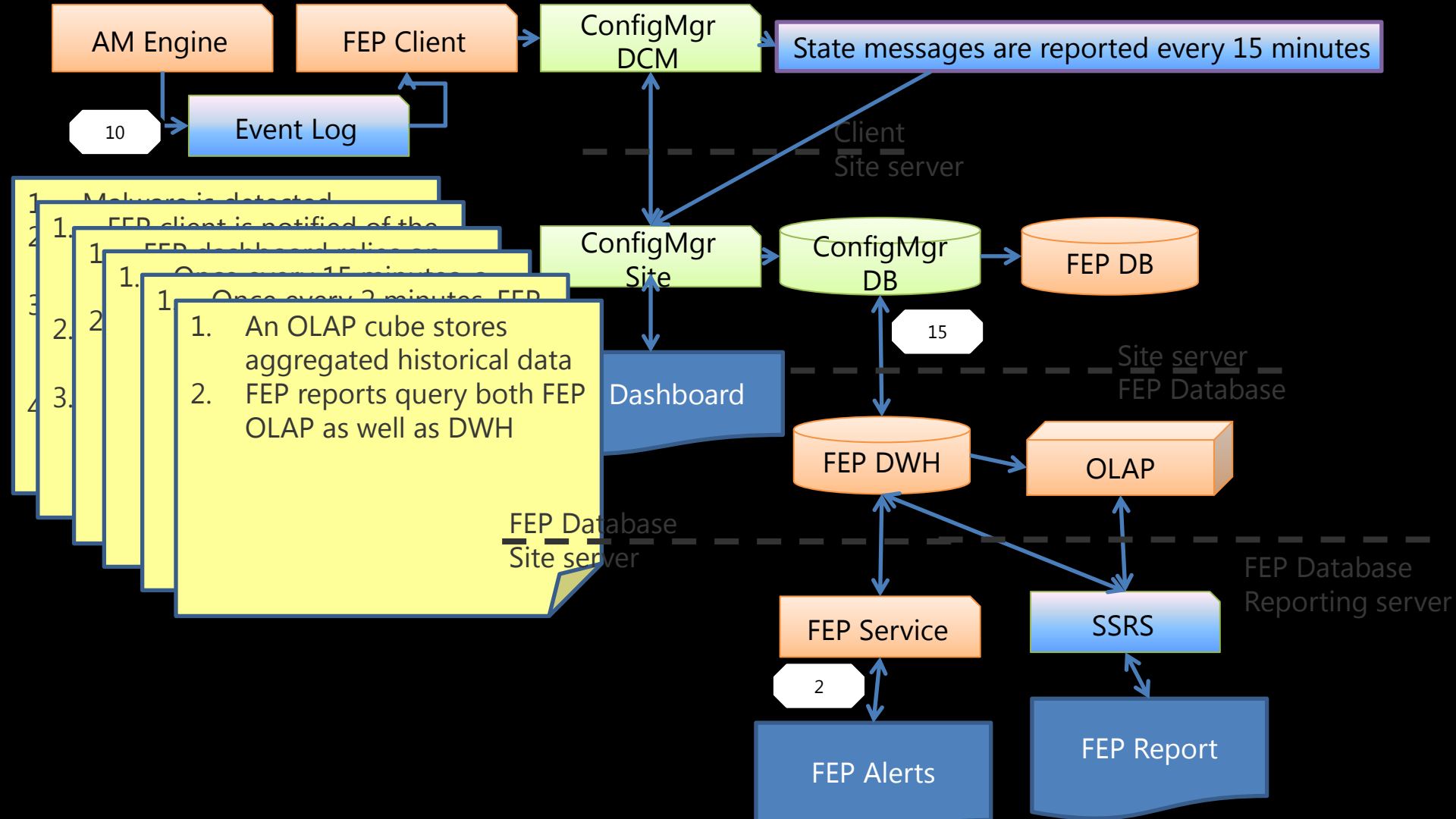
Referens material

- MSFAQ.SE
- www.msfaq.se
- Limited FEP Admin
- <http://social.technet.microsoft.com/wiki/contents/articles/setting-up-a-new-fep-administrator.aspx>
- Capacity Worksheet
- <http://blogs.technet.com/b/clientsecurity/archive/2011/01/19/fep-capacity-planning-worksheet.aspx>
- OSD Install
- <http://blogs.technet.com/b/clientsecurity/archive/2011/01/12/configuration-manager-fep-and-osd.aspx>
- Change retention period in database
- <http://www.msfaq.se/2011/02/fep-changing-retention-period/>
- Deploying KB981889
- <http://blogs.technet.com/b/clientsecurity/archive/2011/01/17/fep-2010-deploying-client-kb981889-ahead-of-time.aspx>
- Forefront Endpoint Protection Forum
- <http://social.technet.microsoft.com/Forums/en-us/FCSNext/threads>

- Malware Protection Center
- <http://www.microsoft.com/security/portal/>
- Security Intelligence Report
- <http://www.microsoft.com/security/portal/>
- AV Comparison
- <http://www.av-comparatives.org/>
- Upgrading FCS to FEP

Dashboard möjligheter





Microsoft®
tech·days
Sweden | 2011