# Keskitetty virustorjunta

F-Secure Policy Management Server

# Tuetut järjestelmät

- Policy Management Server
  - Windows-palvelimet
  - Linux
    - Redhat, Suse, Debian
- Policy Manager Console
  - Windows palvelimet ja työasemat
  - Linux
    - Redhat, Suse, Debian
    - AutoDiscover pohjainen client asennus ei toimi

# F-Secure Policy Management Server

- Komponentit
  - Policy Management Server
    - Hallintapalvelin
  - Policy Management Console
    - Hallintapalvelimen pääkäyttösovellus
  - Automatic Update Agent
    - Virustietokanta-päivitykset
  - Management Agent
    - Hallintapalvelimen Client-ohjelmisto

# Policy Management Server

- Hallinnoi Client-järjestelmien asetuksia
- Mahdollistaa F-Secure-tuotteiden jakelun organisaatiossa
- Keskitettyt päivitykset Client-ohjelmistoihin
- Kerää loki-tiedot Client-järjestelmiltä

# Policy Management Server

- Kansioita
  - CommDir
    - Sisältää koko management-palvelimen hallinta-rakenteen
  - CommDir\Install\Entry
    - Kansiosta ladataan asennettavat ohjelmistot (.jar –paketit)
- Tiedostoja
  - admin.pub, admin.prv
    - Salaus-avaimet, joilla hallinta mahdollista
    - Hallinta-palvelin kohtaiset

# Policy Management Server

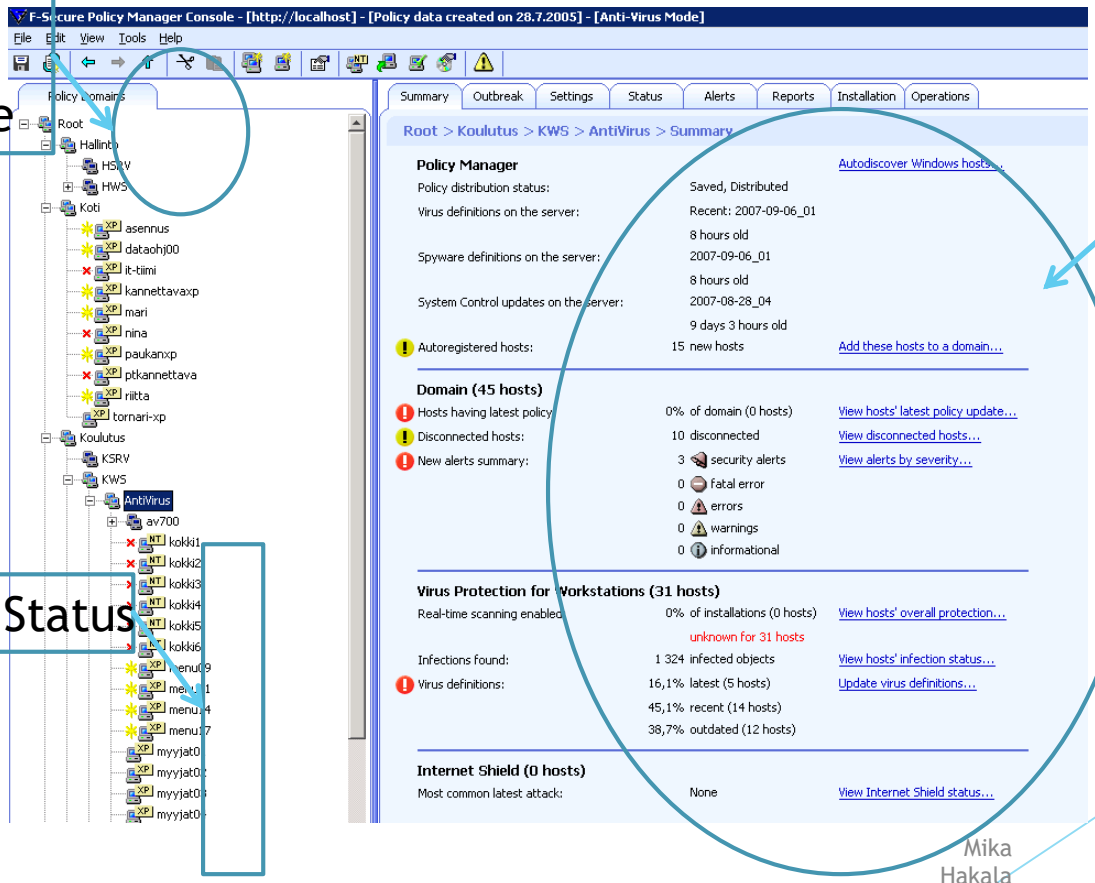
- Asennuksessa huomioitavaa
  - Palvelin sisältää kolme palvelua
    - Host
      - Järjestelmä, jonka kanssa clientit keskustelevat
    - Administration
      - Pääkäyttöliittymän palvelu, otetaan yhteyttä management consolella
    - WebReport
      - Raporttien katseluun, toimii selaimella
  - Asennettavat client-ohjelmistot kannattaa kopioida asennus-ohjelmiston hakemistoon
    - Luodaan hakemisto jars, jonka alle jar-päätteises asennuspaketit kopioidaan
- Palvelimen asennus jatkuu hallinta-konsolin ensimmäisellä käynnistyksellä
  - Luodaan commdir
    - päivitettäessä kysyy vanhan commdir:in sijaintia
  - Rakennetaan salaus-avaimet

# Policy Management Console

- Keskitetyn tietoturva-hallinnan pääkäyttösovellus
  - Toimii myös käyttöliittymänä raporttien lukijoille
- Hallinta-ideologia perustuu Policy Domain rakenteeseen
  - Koneet ryhmitellään domain-rakenteella, joka on puu-rakenne
  - Isäntä-tason asetukset astuvat voimaan lapsissa, ellei lapsitasolla ole erikseen määritelty samaa asetusta
  - Domain-rakenteella ei ole mitään tekemistä verkon rakenteen kanssa
  - Ryhmittely-perusteena erilaisia asetus-kokonaisuuksia vaativat koneet
    - Kannettavat
    - Työasemat
    - Palvelimet
    - Osastot
    - Toimipisteet
- Tuotteella hallitaan useiden eri F-Securen sovellusten asetuksia

# Policy Management Console 2

Policy Domain Rakenne




Järjestelmän tila

Koneen Status

# Policy Management Console 3

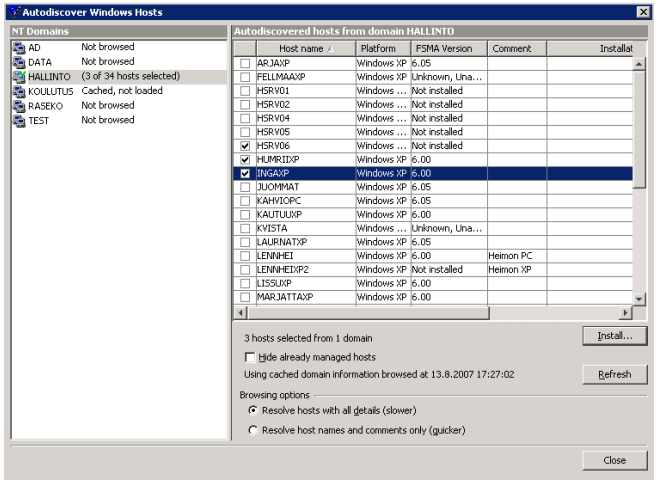
- Vain  yksi pääkäyttäjä kerrallaan voi olla tilassa josta mahdollista tehdä muutoksia
- Lokien seuranta
  - alerts, reports
- Asennukset ja päivitykset
  - Autodiscover, Push
    - Autodiscover etsii verkosta työasemat joihin asennus voidaan tehdä
    - Push mahdollistaa asennuksen tiettyyn ip-osoitteeseen tai koneeseen
  - Installation Packages
    - Asennetut asennus-paketit
    - Asennus-pakettien luonti
  - Asennusten jälkeen pitää muistaa jakaa asetukset uudelleen

# Policy Management Console 4

- Asennuksessa huomioitavaa
  - Palomuuri ei saa estää työaseman ja palvelimen välistä liikennettä
  - Asentajalla pitää olla pääkäyttöoikeudet kohde-koneisiin
  - Windowsin oletus pääkäyttö-jaot pitää olla olemassa kohdekoneilla
    - Admin$ ja system-aseman jako
- Asetusten jakelu
  - policy, distribute
  - muutosten jälkeen pitää muistaa tallentaa ja jakaa asetukset uudelleen
- Asetusten jakelu voi myös sisältää asennustehtävät
  - Kohde-koneissa pitää olla Management Agent
  - Voidaan päivittää ohjelmisto-versioita ja asentaa hotfix-päivityksiä

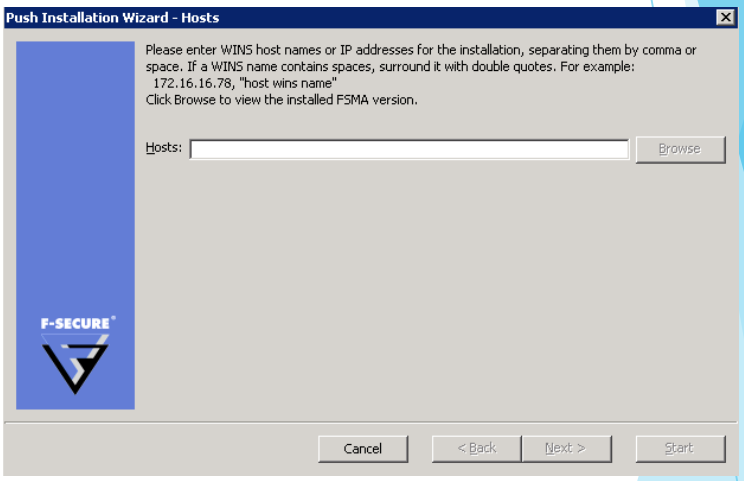
# Torjunta-ohjelman jakelu

- Asennuksessa voidaan käyttää Auto-Discover toimintoa
- Näyttää koneet verkon työryhmien / domainien alla
- Asennettavat koneet valitaan rastittamalla
  - Yhdessä asennustehtävässä voi asentaa vain yhtä tuotetta



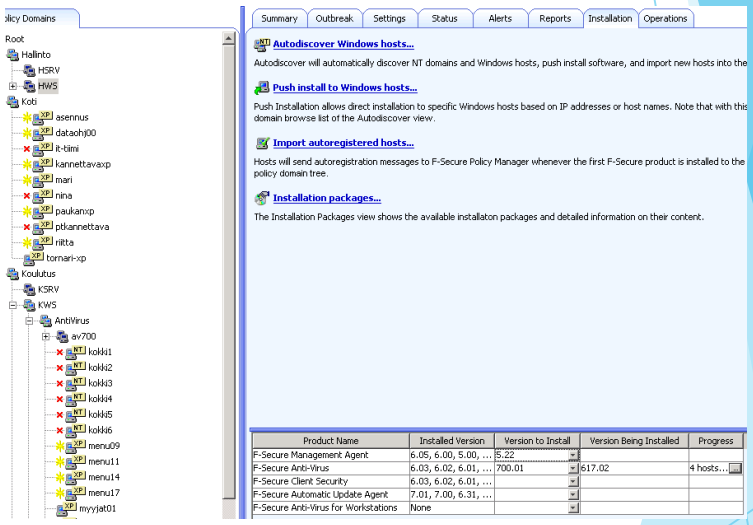
# Torjunta-ohjelman jakelu 2

- Tarvittaessa voidaan käyttää manuaali-asennusta
  - Annetaan koneen tai koneiden ip-osoitteet / koneen nimet
- Asennuksen jälkeen asetukset pitää jakaa uudelleen



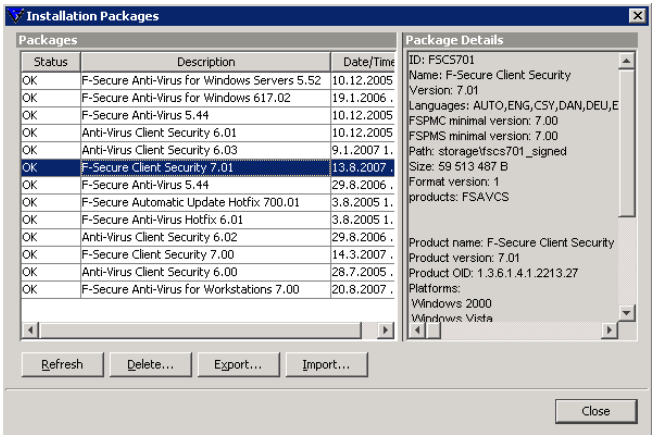
# Ohjelmapäivitykset

- Ohjelmisto-päivityksiä voidaan tehdä Management Agentin avulla
  - Versio-päivitykset
  - Korjaus-päivitykset



# Ohjelmistojen lisääminen hallintapalvelimeen

- Lataus internetistä
  - http://www.f-secure.com/webclub
  - Jar-paketit on tarkoitettu hallinta-palvelimelle
- Import-toiminnolla voidaan tuoda ohjelmisto-paketteja
  - Myös commdir-hakemiston entry kansiota voidaan käyttää
- Export-toiminnolla voidaan luoda automaatti-asennus-paketteja
  - Tukee myös MSI-paketteja



# Management Agent

- Käyttää oletuksena liikenteeseen tcp-protokollan porttia 80
- Client-koneissa määritelty Management Server:in osoite
  - Esim. http://f-secure.firma.com:80/
  - Porttia ei tarvitse mainita jos palvelin käyttää oletusporttia
- Management Agent rakentaa koneelle yksilöllisen id-numeron, jonka avulla hallinta-palvelin tunnistaa koneen
  - ID-numero voidaan generoida uudelleen
    - Fsmautil resetuid
      - Sovellus löytyy f-securen asennushakemistosta common-kansiosta
  - Id on generoitava uudelleen esim. konetta monistettaessa
    - Muuten samalla id:llä olevat koneet näkyvät hallinta-palvelimessa yhtenä koneena

# BackWeb / Automatic update agent

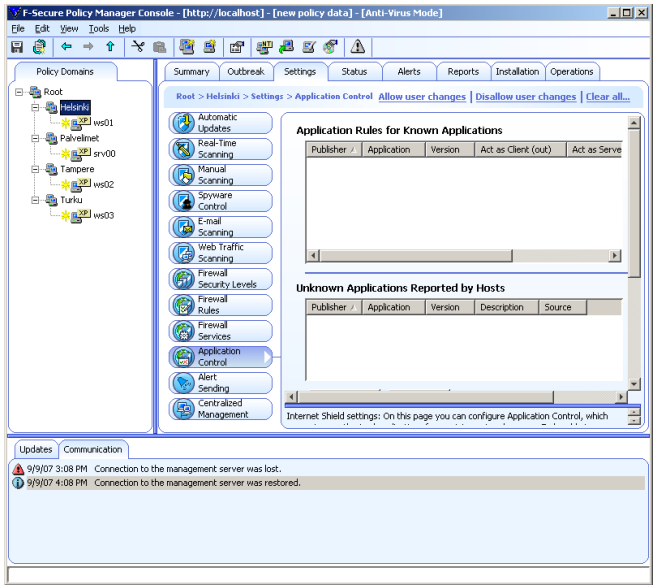
- Voidaan asentaa sekä Client-koneille että pelkästään hallinta-palvelimelle
  - Automatic update agent asentuu automaattisesti client-järjestelmiin
- Hakee virus-tietokanta-päivitykset F-Securelta automaattisesti
  - Päivittää Client-järjestelmän virustietokannat suoraan
    - TAI
  - Management Server jakelee päivitykset Client-järjestelmille

# Virustorjunnan asetukset

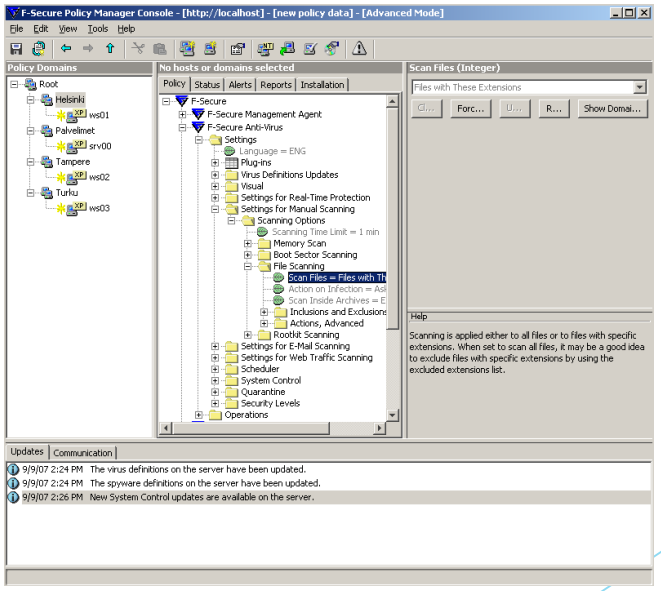
- Management consolessa kaksi toimintatilaa
  - Anti-Virus mode
    - Suurin osa asetuksista voidaan määritellä tässä tilassa
  - Advanced mode
- Asetukset voidaan määritellä
  - Policy domain-kohtaisesti, asetukset periytyvät puurakenteessa
  - Konekohtaisesti, jos tarvetta on

# Hallintakonsolin toimintatilat

## Anti-virus tila




## Advanced tila



# Virustorjunnan asetukset

- Voidaan  määritellä halutut toiminta-tavat
  - Voidaan myös määritellä automaatti-toimenpiteet hälytys-tilanteissa
- Reaaliaikainen torjunta
  - Määritellään halutut tiedostopäätteet ja seurannan kohteet
  - Määritellään kohteet, joita ei tarkisteta
    - Sovellukset, hakemistot
    - Verkkolevyt
- Manuaalinen torjunta
  - Määritellään asetukset käyttäjän itse aloittamaan virusterkistukseen

# Virustorjunnan asetukset 2

- Vakoiluohjelmisto suojaus
  - Määritellään halutut toimenpiteen vakoiluohjelmistoja varten
- Sähköposti-tarkistus
  - Määritellään lähtevän ja saapuvan postin tarkistus
  - Toimintatavat hälytyksen sattuessa
- http-liikenteen tarkistus
  - Määritellään http-liikennettä koskevat tarkistussäännöt

# Palomuuri-konfiguraatio

- F-Securen palomuurin asetukset koostuvat useista osista
- Pää-asetukset on jaettu alueisiin
  - Jokainen alue sisältää omat säännöstöt
  - Alueina: Mobile, Home, Office Strict, Normal, Custom, Disabled, Network Quarantine
  - Käyttäjä voi valita alueen sen mukaan, minkälaiseen verkkoon hän on kytkeytyneenä
  - Disabled poistaa palomuurin pois käytöstä
  - Network Quarantine aktivoituu, jos virustunnisteet riittävän vanhoja
    - Reagointi-ajan voi määritellä
- Muissa osissa määritellään varsinaiset palomuuri-säännöt
  - Services / Palvelut
    - Määritellään verkkoliikenne-tapahtumaan liittyvä ip-liikenne
  - Rules
    - Määritellään palveluun liittyvä sääntö

# Palomuuri-konfiguraatio 2

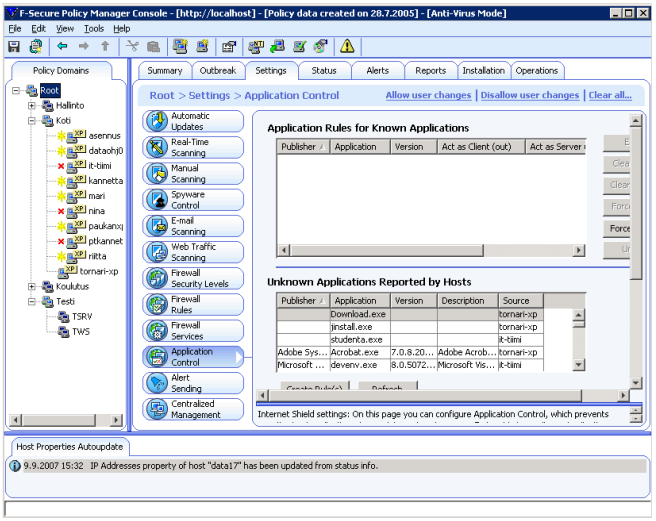
- Palvelun määrittely
  - Palvelun nimi ja kuvaus
  - IP-protokolla
    - Tcp, udp, icmp, gre…
  - Lähtöportti
  - Kohdeportti
  - Liikenteen luokka
    - Määritellään liikenteen luokittelu F-Securen mukana olevilla perus-luokituksilla
    - Informatiivinen

# Palomuuri-konfiguraatio 3

- Palomuurisäännön määrittely
  - Valitan muokattava sääntöalue
  - Kieltävä (Deny) tai myöntävä (Allow) sääntö
  - Liikenteen toinen osapuoli
    - Mikä tahansa, paikallisen verkon koneet, tietyt järjestelmät
  - Määritellään palvelu(t) ja liikenteen suunnat
    - Listassa voidaan määritellä useita palveluja
    - Hyödyllistä esim. lähiverkon sallittuja palveluja määriteltäessä
  - Onko sääntö voimassa vain soitto-yhteydessä
    - Perinteinen modemi-yhteys, vpn
    - Hälytys-käytäntö
  - Säännön kuvaus
- Säännön lisäämisessä pitää olla tarkka (Before / After)
  - Sääntölistaa luetaan ylhäältä alaspäin

# Sovellusten hallinta

- Sovellusten hallinnassa on mahdollista määritellä verkkoa käyttävien sovellusten liikenne-oikeuksia
  - Client
    - Lupa liikennöidä ulospäin
  - Server
    - Lupa vastaanottaa liikennettä
- Järjestelmä kerää Management clienteilta tietoja käytössä olevista sovelluksista
  - Pääkäyttäjä voi määritellä kerätyn tiedon perusteella sallitun politiikan
- Oletuksena ohjelmisto kysyy käyttäjältä, mitä tehdään
  - Yritys-järjestelmissä yleensä asetukset kiinnitetty
- Sovellusten hallinta liittyy muuhun palomuurikonfiguraatioon



# Hälytykset

- Järjestelmä kerää status-informaatiota client-systeemeistä
- Hälytykset lähetetään hallinta-palvelimelle
  - Hälytyksessä aika, kone, käyttäjä-tiedot ja hälytyksen aiheuttama tapahtuma
- Pääkäyttäjän tehtävä on seurata hälytyksiä ja päättää jatkotoimenpiteet
  - Etenkin käyttäjille tapahtuvaa tiedotusta pitää miettiä
- Hälytyksissä kannattaa aina miettiä, tarvitaanko todellisia toimenpiteitä

# Järjestelmän asetukset

- Tools-valikon Reporting valinnalla voi generoida laajan raportin
  - Raporttiin tulevia asioita voidaan säätää
- Tools-valikon Preferences-valinnalla voidaan säätää hallintapalvelun asetuksia
  - Kuinka usein hallintanäkymä päivittyy
  - Koska virustietokannat ovat liian vanhoja
  - Raporttien ja hälytysten poisto-asetukset
  - Policy-tiedostojen optimointi

# Yleisiä periaatteita

- Reaaliaikainen virussuojaus käytössä kaikissa työasemissa
  - Tarkistettavien tiedostojen listaa pitää välillä päivittää, etenkin tiedostopäätteitä
- Palomuuri käytössä kannettavissa koneissa
  - Tarvittaessa kytketään myös työasemiin
  - Sovelluskontrollin määrittely kohdalleen vie aikaa
- Palvelinten virustorjunta mietitään tarpeen mukaan
- Sähköpostipalvelimissa yleensä oma virustorjunta ja spam-suodatus