

SAFETICA KURULUM KILAVUZU

SAFETICA KURULUM KILAVUZU

Safetica 5.0.4 versiyonu için

Safetica, Safetica Technologies tarafından geliştirilmiştir

Tüm hakları saklıdır. Yazarından yazılı izin alınmaksızın çoğaltılamaz, saklanamaz, dağıtılamaz.

Belgenin yazarı ve dağıtıcıları bu belgenin hazırlanmasından kaynaklanan hata, eksiklik ve hasarlardan dolayı sorumlu tutulamaz.

Daha fazla bilgi için www.fins.com.tr adresimizi ziyaret edin.

Yayın tarihi: 2013

ÇER K

Giri

SAFETICA

1	Yapı	5
2	Gereksinimler	7
	Safetica Management Service	7
	Safetica Management Console	8
	Safetica Endpoint Client	8

SAFETICA KURULUMU

1	Standart kurulum	9
	Before installation	10
	Creating Microsoft SQL server databases	12
	Installation of Safetica Management Service	14
	Installation of Safetica Management Console	16
	Configuration of Safetica Management Service	16
	Installation of Safetica Endpoint Client	20
	Installation using GPO	21
	After installation	25
2	Küçük kurulum	27
	Before installation	28
	Installation of Safetica Management Service	28
	Installation of Safetica Management Console	30
	Configuration of Safetica Management Service	30
	Installation of Safetica Endpoint Client	33
	After installation	34

İNDEKS

0

1 Giri

Sevgili kullanıcı,

Firmanızı korumak için Safetica yazılımını seçtiğiniz için teşekkür ederiz. Bu kılavuzda sizi kurulum için tüm aşamalarda adım adım yönlendirecek anlatım bulabilirsiniz. Kurulumda problem yaşarsanız, *öncelikle Detaylı Safetica Kılavuzuna başvurunuz*. Bundan sonra halen probleminiz devam ediyorsa www.fins.com.tr adresimizden bizimle iletişime geçebilirsiniz.

Safetica iç güvenliğe tamamen yeni bir yaklaşım sunar. Bu ürün gerçek korumayı iç koruma ile birleştiren ilk üründür. Kullanıcıları izleyerek riskleri açığa çıkarır ve istenmeyen davranışları engellemesi and veri sızmasına karşı özellikleri (DLP) ile firmayı çalışanların istenmeyen aktivitelerinin sonuçlarına karşı korur.

Ürünün başarılı kurulumu için *Detaylı Safetica Kılavuzunu* okumanızı öneririz. Burada başlangıç dağıtımından, kullanım örneklerine kadar bir çok konuda detaylı bilgiye ulaşabilirsiniz.

Temel uygulamalar ve kullanımda çabucak ustalaşmak için *Safetica quick wizard'ı kullanabilirsiniz*. Yazılımın kullanımı hakkında kullanıcıların sıkça sordukları soruların cevapları *Frequently asked technical questions of Safetica users kısmında bulunabilir*.

Teşekkürler,

2 SAFETICA HAKKINDA

Firmanız her gün çalışanlarınız tarafından zarar görebilir. Çalışıyor görünebilirler, firma kaynaklarını yanlış kullanabilirler ya da hassas verinizi çalıp çaldırabilirler. Safetica güvenlik yazılımı firmanızı tüm bilinen çalışan hatalarına karşı koruyabilecek dünyadaki tek çözümdür: hassas veri sızması, finansal kayıplar ve firmanızın itibarının zedelenmesi. Aynı zamanda, sizi çalışanlarınızın tehlikeli davranışları hakkında zarar oluşmadan çok önce uyararak önlem almanız için size zaman kazandırır.

Ba lıca Faydaları

- Firmanızı çalışanlarınızın hatalarının bedelini ödemekten korur.
- Tehlikeli çalışan davranışlarını zamanında tespit eder.
- Çalışanlarınızın iş aktiviteleri ve üretkenliklerinden haberdar olmanızı sağlar.
- Hassas firma verilerinizin ait oldukları yerde -içeride- kalmasını garantiler.
- Firmanızın çıkarlarını çalışanlarınızın mahremiyetini göz ardı etmeden korur.
- Personelinizin hassas verinize sadece izin verdiğiniz şekilde erişimini garantiler.
- Firmanızın günlük işlerini aksatmadan sizi korur.
- Endüstriyel kısıtlamalar, düzenlemeler ve yasalarla uyumludur.

Safetica Modülleri

Auditor

Potansiyel olarak tehlikeli çalışan davranışlarının oluşmadan farkına varır. Personelinizin

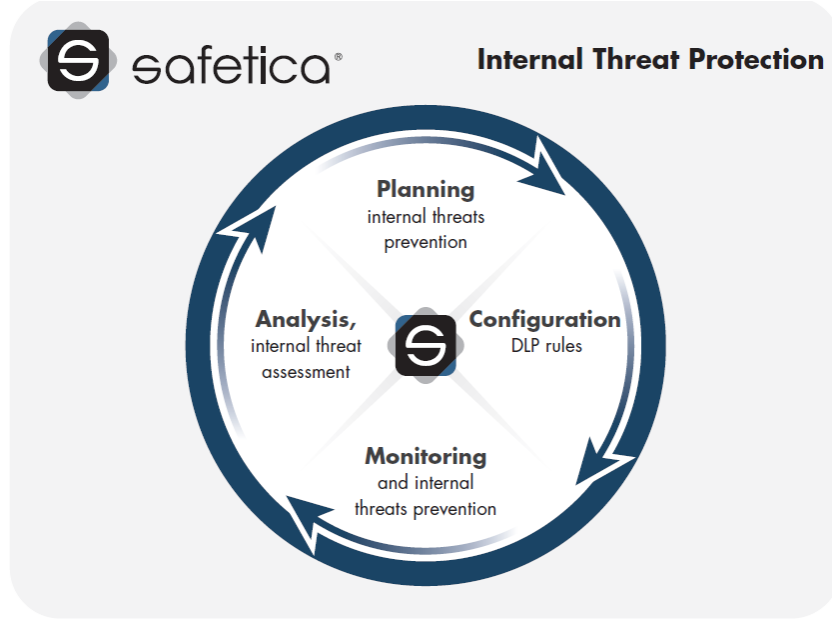
iş aktivitesini izler ve kimin firmanıza zarar vermek istediğini gösterir.

DLP

Çalışanlarınızın erişmelerine izin verdiğiniz veriyi yanlış kullanmalarını önler ve hassas firma verinizi yetkisiz erişimden korur.

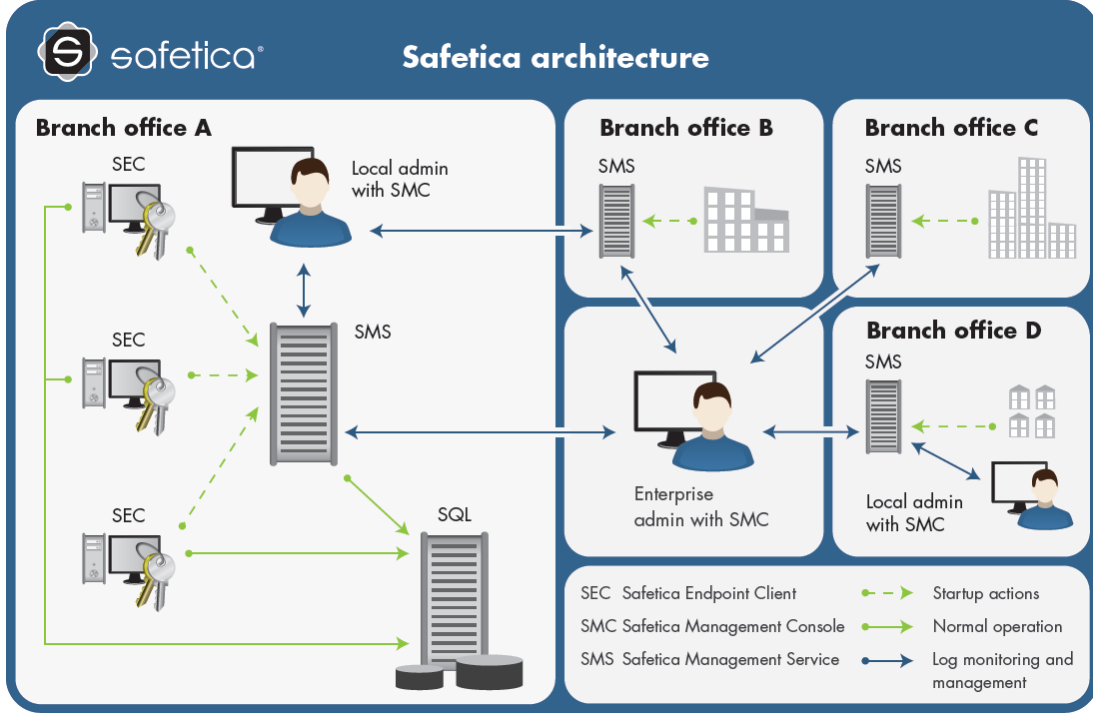
Supervisor

Çalışanlarınızın iş aktivitelerini kontrol edin. İstenmeyen davranışları engelleyin ve böylece üretkenliği artırın.



2.1 Yapı

Safetica sunucu-istemci yapısı ile kurulmuştur. İstemci uygulama Safetica Endpoint Client (SEC) iş istasyonları üzerinde çalışır. Bu uygulama Safetica Management Service (SMS) sunucu bileşeni ile iletişim kurar. Güvenlik yetkilileri ya da yöneticiler uzak bağlantı için Safetica Management Console (SMC)'u kullanabilir. İş istasyonlarının izlenmesi ile elde edilen veri veri tabanı sunucusunda depolanır. Yazılım kapsamlı ağları hatta çok uluslu ağları bile destekleyecek şekilde optimize edilmiştir.



Böylelikle Safetica merkezi olmayan bir çözümdür. Birden fazla sunucuyu tek konsoldan yönetmenize olanak tanır (tabi ki bağımsız yönetim de mümkündür). Her bir sunucu firma ortamının bir kısmına hizmet verebilir, böylelikle yükü bölmek de mümkün olur. Bu yapı ile birden fazla kolu ve aslında sınırsız kullanıcıyı ve bilgisayarı desteklemek mümkündür.

Aşağıdaki bileşenlerden her biri farklı bir bilgisayar üzerine kurulabilir.


SMS sunucu kısmını temsil eder. Sunucuda servis olarak çalışır. Bir domain üzerinde birden fazla servis çalışabilir. Küçük ağlar için bir seçenek de servisi domain olmayan bir ağ üzerine kurmaktır. Böylece servis standart bir bilgisayar üzerinde çalışabilir.

Her bir Safetica Management Servisi üzerinde ayrı ayrı yöneticilere Safetica Management Console kullanarak farklı yetkiler verilebilir ve böylelikle firma güvenlik kontrolü farklı rollere bölünebilir (örn. yerel admin, genel admin, güvenlik müdürü, vb.).

SMC istemci istasyonlarının , sunucu servislerinin ve veri tabanlarının ayarlanması ve kontrolünü sağlayan bir yönetim merkezidir. SMC ayrıca izleme, istatistikler ve grafiklerin de görüntülenebildiği yerdir. Konsol kurulumlarının ve kullanıcılarının sayısı lisansla sınırlı değildir.

SEC her bir çalışanın iş istasyonunda çalışan istemci bileşeni temsil eder. İki ana kısım içerir:

- Safetica Client Servisi – işletim sisteminin her başlangıcında servis olarak çalışır ve izleme, ilkeleri uygulama ve veri tabanı ve Safetica Management Servisi ile iletişimi sağlama işlerini gerçekleştirir. Client servisi Auditor, DLP ve Safetica Endpoint özelliklerinin kullanıcı bilgisayarlarında işlemlerini sağlar.
- Endpoint Security Tools – güvenlik araçları içeren bir kullanıcı arayüzü. Bu kısım yalnızca geçerli bir DLP modülü lisansı ile kullanılabilir. Ayarlara göre üç modda çalışabilir:

1. Endpoint Security Tools – bildirim alanındaki  simgesine sağ tıklayarak açılabilen kullanıcı arayüzü (DLP lisansı gerektirir).
2. Gizli mod - temel kullanıcı işlevleri içerir kullanıcı arayüzü içermez (DLP lisansı gerektirir).

3. Endpoint Security Tools ve menü içermeyen görünmez mod. İstemci üzerinde yalnızca servis çalışır. Bu mod SEC servisini kendi başına gizlemez. Gizleme işlemi Endpoint Security Tools ayarları içerisinde gerçekleştirilebilir.

SQL database son kısımdır ve izleme verisi ve ayarlar için depolama yapar. Bu bileşen de uygulamalar, siteleri ve uzantılar içeren bir kategori veri tabanıdır. Aşağıda database engine'lerin kullanımı ile Standart ve Küçük kurulumun arasındaki fark anlatılmıştır.

- Standart kurulum:
 - SEC, logları, ayarları ve kategorileri geçici olarak tutmak için SQLite database kullanır.
 - SMS ana veritabanları için Microsoft SQL Server platformu kullanır.
 - . SMS kurulumundan önce MS SQL server kurulmuş ve yapılandırılmış olmalıdır. SMS yapılandırılırken üç veri tabanı otomatik olarak oluşturulur.
- Küçük kurulum:
 - SEC, logları, ayarları ve kategorileri geçici olarak tutmak için SQLite database kullanır.
 - SMS, ana veritabanları için SQLite kullanır. Veritabanları otomatik olarak oluşturulur ve SMS ile aynı makine üzerinde konumlandırılır.

Veri Hesaplayıcı

Veri hesaplayıcı SQLite ya da MS SQL veri tabanının Safetica yazılımını çalıştırmak için ihtiyaç duyacağı yaklaşık disk boyutunu hesaplar. Kullanıcı sayısını, kullanıcı aktivite seviyesini, ekran görüntüsü kalitesini ve tercih edilen modülleri seçerek, kolayca paylaşılabilir veri tabanı kapasitesi hesaplamaları elde edebilirsiniz.

Hesaplayıcı web sitemizde bulabilirsiniz. www.fins.com.tr

Not

Yukarıda tarif edilen bileşenlerin tamamı aynı makineye kurulabilir ancak güvenlik ilkeleri ayarlarına bağlı olarak, SMS ve SMC performansı olumsuz etkilenebilir. Örneğin, makine üzerinde ağ bağlantısını etkisiz hale getirirseniz, diğer SEC'ler SMS'e bağlanamayacaktır.

2.2 Gereksinimler

Yapı kısmında anlatıldığı üzere, Safetica her biri farklı özelliklere sahip çeşitli bileşenlerden oluşur. Bu bileşenlerin her biri kendine has işletim sistemi, donanım ve yazılım gereksinimlerine sahiptir.

Aşağıdaki kısım Safetica bileşenlerinin gereksinimlerini anlatmaktadır.

2.2.1 Safetica Management Service

Tavsiye Edilen Donanım Gereksinimleri

- 2.4 gigahertz (GHz) 32-bit (x86) ya da 64-bit (x64) dual-core işlemci
- 2 GB RAM
- 10 GB hard disk alanı

Minimum donanım gereksinimleri

- 1.8 gigahertz (GHz) 32-bit (x86) ya da 64-bit (x64) single-core işlemci
- 1 GB RAM
- 4 GB hard disk alanı

Yazılım gereksinimleri

- Geniş network ([Standard kurulum](#)) – paylaşılmış ya da adanmış bir sunucu, gerekirse, geniş ağlar için çoklu sunucular. İşletim Sistemleri: MS Windows Server 2003 SP1, 2003 R2, 2008, 2008 R2, 2012 32-bit ya da 64-bit, domain ve Active Directory, aşağıdaki veri tabanlarından birinin kurulumu gerekir:
MS SQL 2008, 2008 R2, 2012 Express edition ve 32-bit ya da 64-bit dahil. (Express edition'ın Advanced Services ile olması tavsiye edilir.)
- Küçük network ([Küçük kurulum](#)) – yazılım tek bir makina üzerinden çalışabilir ve 20 bilgisayara kadar olan küçük firmalarda yeterli olabilir. Bu aşağıdaki işletim sistemlerini destekler: MS Windows XP SP2, Vista, 7, 32-bit veya 64-bit. The SQLite database kullanılır; bu database ayrı kurulum istemez.

Database izlemeden, ayarlardan ve loglardan elde edilen verilerin depolanması için kullanılır. Ayrıca web sayfalarının, uygulamaların ve uzantıların kataloglarını depolar.

2.2.2 Safetica Management Console (Yönetim konsolu)

Tavsiye edilen donanım gereksinimleri

- 2.4/1.6 gigahertz (GHz) 32-bit (x86) ya da 64-bit (x64) single/dual-core işlemci
- 1 GB RAM
- 2 GB hard disk alanı

Minimum donanım gereksinimleri

- 1.5 gigahertz (GHz) 32-bit (x86) ya da 64-bit (x64) single-core işlemci
- 512 MB RAM
- 2 GB hard disk alanı

Yazılım gereksinimleri

Safetica Management Console herhangi bir yere kurulabilir. Aşağıdaki işletim sistemlerini destekler: MS Windows XP SP3, Vista, 7, 32-bit ya da 64-bit (SMS için belirtilen sunucu işletim sistemlerine de kurulum yapılabilir).

2.2.3 Safetica Endpoint Client (Istemci)

Tavsiye edilen donanım gereksinimleri:

- 2.4/1.6 gigahertz (GHz) 32-bit (x86) ya da 64-bit (x64) single/dual-core işlemci
- 1 GB RAM
- 2 GB hard disk alanı

Minimum donanım gereksinimleri

- 1.5 gigahertz (GHz) 32-bit (x86) or 64-bit (x64) işlemci
- 512 MB RAM
- 2 GB hard disk alanı

Yazılım gereksinimleri

Safetica Endpoint Client kullanıcı bilgisayarlarında kurulur. Aşağıdaki işletim sistemlerini destekler: MS Windows XP SP3, Vista, 7, 32-bit ya da 64-bit. Geniş ağlar için, MS installer paketi gereklidir.

3 SAFETICA KURULUMU

Öncelikle, hangi kurulum türünün kullanılacağı seçilmelidir. Yerleşim boyutunuza göre kurulum türünüzü belirleyebilirsiniz.

İki farklı kurulum türü mevcuttur.

- [Küçük Kurulum](#) – küçük işletmeler için uygundur. Setup ile birlikte gelen SQLite database kullanır. Tek bir sunucu bileşeni (Safetica Management Service) 20 client'a kadar yönetebilir (Safetica Endpoint Clients).
- [Standart Kurulum](#) – büyük işletmeler için uygundur. Microsoft Active Directory ile senkronizasyonu destekler. Kurulum MS SQL database kullanır (dahili değil). Tek bir sunucu bileşeni (Safetica Management Service) 20'den fazla client (Safetica Endpoint Clients) için kullanılabilir.

Not

Safetica'nın farklı bileşenlerini kurarken, bileşenleri aynı tür kurulum menüsünden seçmeye dikkat ediniz.

3.1 Standard kurulum

Standart kurulum büyük işletmeler düşünülerek hazırlanmıştır. Microsoft Active Directory ile senkronizasyonu destekler. Veri depolama için MS SQL database kullanılır (kurulumu dahil değil). Bir sunucu bileşeni (Safetica Management Service) 20'den fazla client (Safetica Endpoint Clients) için yeterlidir. Safetica Management Service'in birden fazla örneği birlikte çalışabilir.

Standart kurulumu yaparken izlenecek yol:

1. Kurulumu başlamadan önce, ağınızın [belirtilen servis gereksinimleri](#)'ni karşıladığından emin olun.
2. Dilediğiniz bilgisayar(lar) üzerine [Safetica Management Service'i](#) kurun. Ayarlar ve kayıtlar için merkezi database otomatik olarak aynı bilgisayar(lar) üzerine kurulacaktır.
3. Safetica'yı yönetmek istediğiniz bilgisayar üzerine [Safetica Management Console'u](#) kurun.
4. Safetica Management Console'u kullanarak, Safetica Management Service'e bağlanın ve [server'ı](#) yapılandırın.
5. Clientlere [Safetica Endpoint Client'ı](#) kurun.

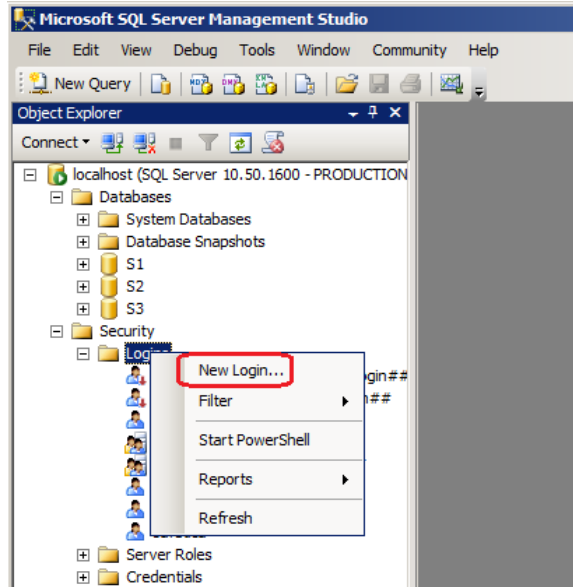
6. **Başlangıç kurulumunu yapın** ve tüm bileşenlerin doğru kurulduğundan ve birbirleriyle doğru bir şekilde haberleştiğinden emin olun.

Tüm bileşenleri kurduktan ve hepsinin doğru kurulduğundan emin olduktan sonra Safetica'yı kullanmaya başlayabilirsiniz.

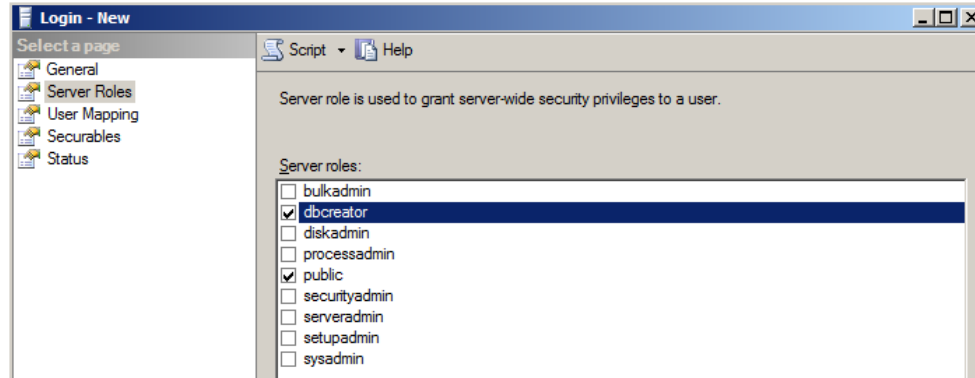
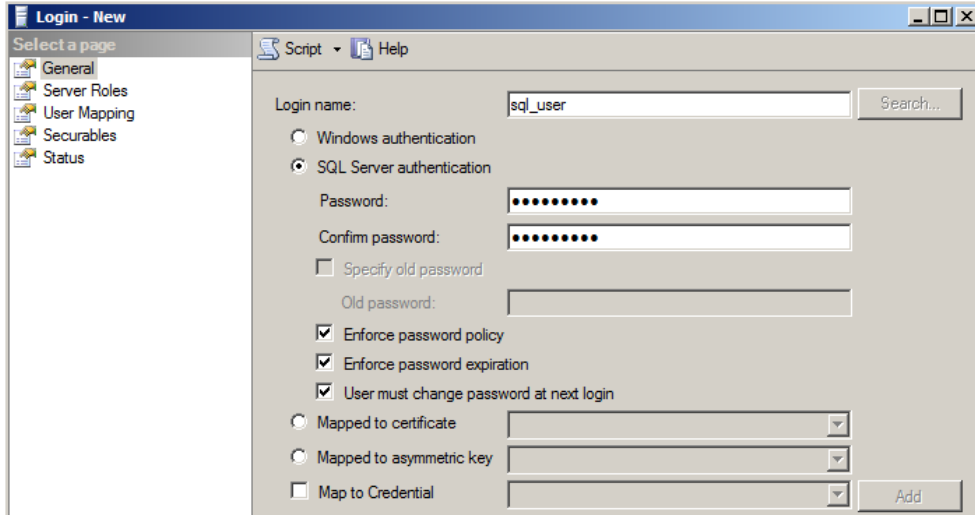
3.1.1 Kurulumdan Önce

Asıl kurulumdan önce aşağıdaki adımları tamamladığınızdan emin olun:

1. Donanım ve **yazılım gereksinimleri**'ne uyumu için Safetica'nın her üç bileşenini de kontrol edin.
2. Kurumsal ağınızda bir ön analiz yapın:
 - o Safetica Management Service, Management Console ve Endpoint Client bileşenlerini sırasıyla ağınızdaki hangi bilgisayarlara kurmak istediğinize karar verin.
 - o Üzerinde merkezi veri tabanları olacak MS SQL sunucusunu belirleyin. Safetica Management Service'in her örneği üç database oluşturur – biri ayarlar, diğeri kayıtlar ve üçüncüsü kategoriler için.
 - o Bileşenlerin hepsini aynı ağdaki bilgisayarlara kurduğunuzdan ve birbirlerine erişebildiklerinden emin olun. Safetica Management Service, database'i, ve Safetica Management Service'e bağlı tüm client'ler birbirlerinden ulaşılabilir olmalıdır. Safetica Management Console sadece Safetica Management Service'e erişmek için haklara ihtiyaç duyar.
3. Microsoft SQL Server'da, SQL Server authentication mode'da database oluşturma hakkına sahip bir kullanıcı oluşturun. Desteklenen Microsoft SQL Server'lar Gereksinimler kısmında bulunabilir.



3. **Install Safetica Management Console** on the computer from which you would like to manage Safetica.

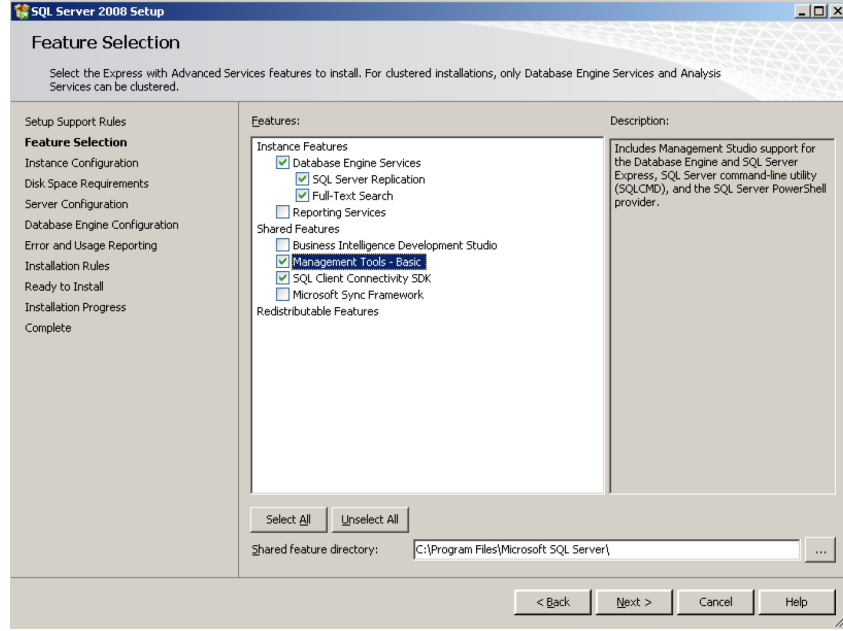


4. Antivirus yazılımınıza ve firewall'unuza izinler tanımlayın ve Microsoft SQL Server'ın doğru yapılandırıldığından emin olun:
 - Safetica Management Service kuracağınız bilgisayarda STAService.exe işlemi için ve aşağıdaki portlar için izinler tanımlayın:
 - 4438 (SEC 'nin SMS ile iletişimi).
 - 4441 (SMC 'nin SMS ile iletişimi).
 - Safetica Management Console kuracağınız bilgisayarda STAConsole.exe işlemi için izinler tanımlayın.
 - Safetica Endpoint Client kuracağınız bilgisayarlarda şu işlemler için izinler tanımlayın: STCService.exe, STMonitor.exe, STUserApp.exe, Safetica.exe, STPCLock.exe.
 - Databases kurulacak bilgisayarda port 1433 için izin tanımlayın.
 - Microsoft SQL authentication mode'un Mixed Mode (Mixed Mode – SQL Server authentication and Windows authentication) olduğundan emin olun.
5. Safetica'nın son versiyonunu içeren kurulum paketini indirin.
 - Kurulum paketi Standard kurulum için gerekli tüm bileşenleri içerir.

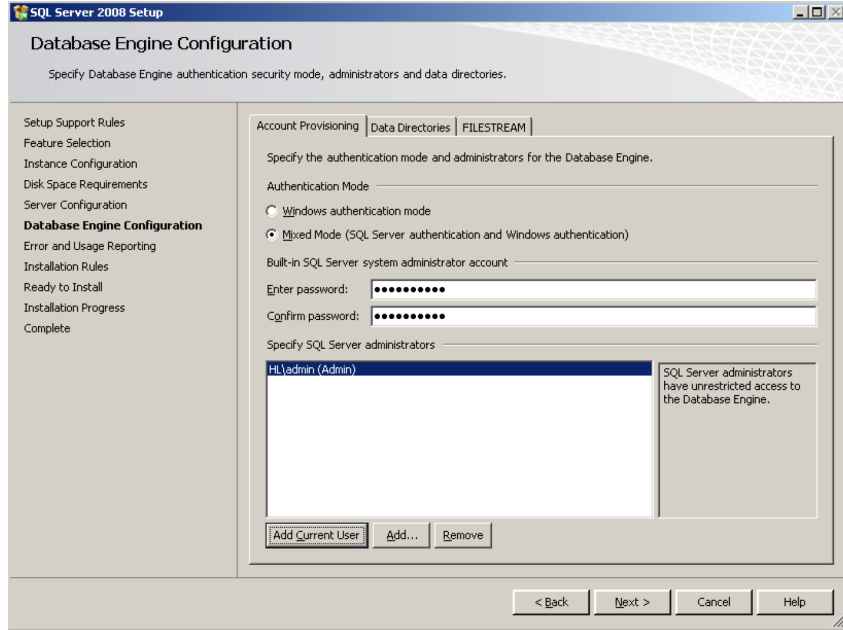
3.1.1.1 Microsoft SQL server databases oluşturma

Standard kurulumdan önce üç temel database için Microsoft SQL sunucu kurulmalıdır. İlk database'e tüm ayarlar kaydedilecek, ikincide izleme kayıtları depolanacak ve üçüncüsü uygulamalar websiteler ve uzantılarla ilgili uzantıları içerecektir.

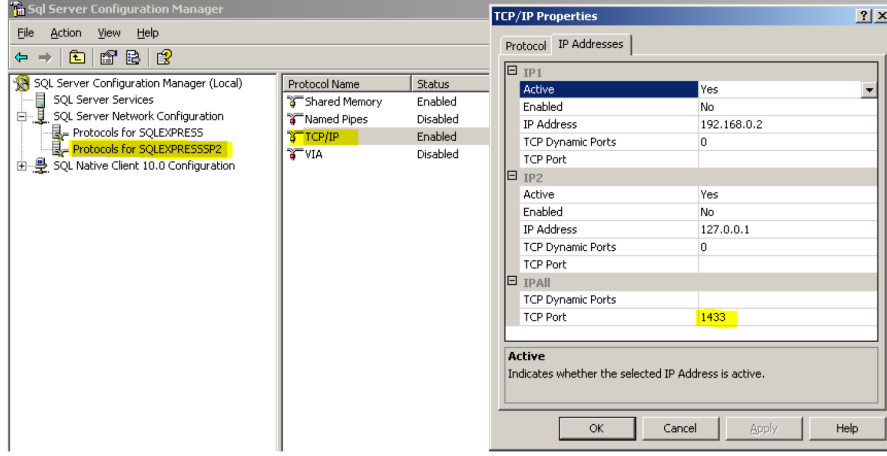
1. MS SQL'i aşağıdaki bileşenlerle sunucunuza kurun.



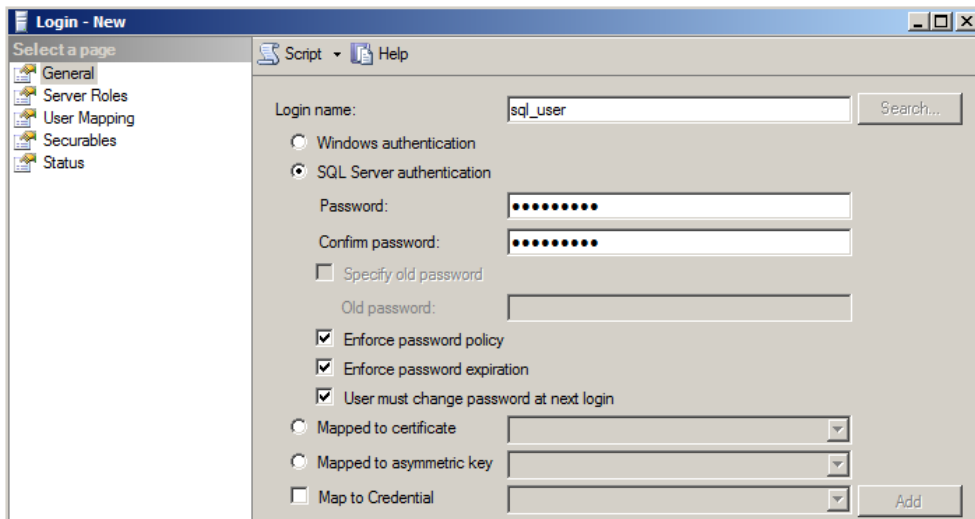
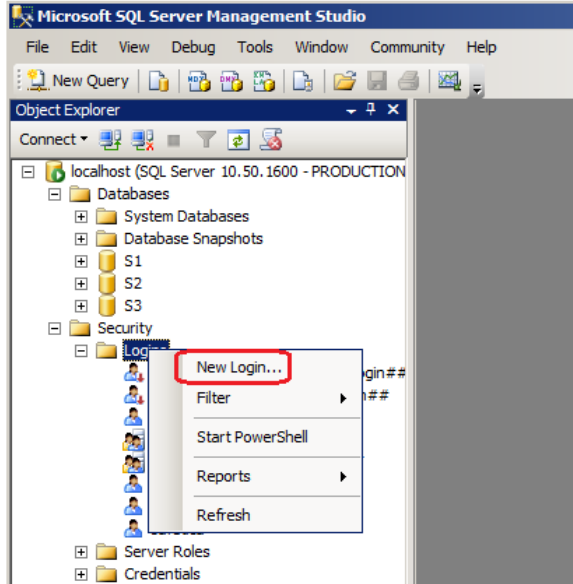
2. İlgili adımda "Mixed mode authentication" seçin.

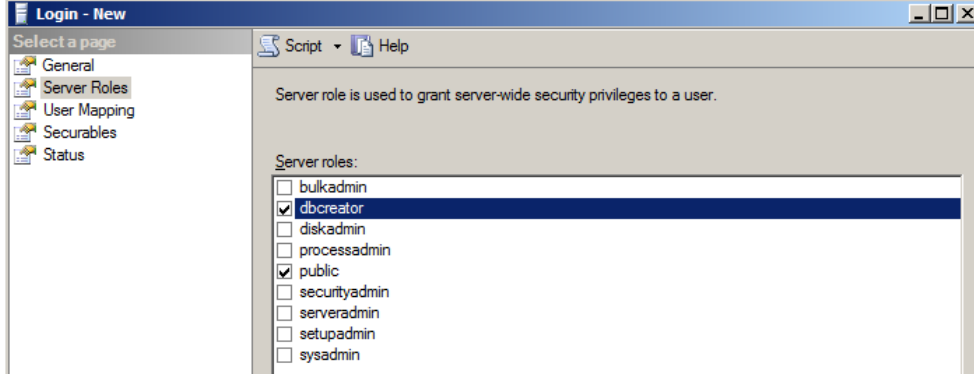


3. MS SQL sunucunun örneğin port 1433'ü dinlediğinden emin olun. Sql Server Configuration Manager aracı ile bu ayarı yapabilirsiniz.



4. Database oluşturmak için yeterli haklara sahip bir MS SQL kullanıcısını Ssql Server Management Studio aracı ile oluşturun. Oturum açma türünü "SQL Server authentication" olarak belirleyin ve yeni bir parola girin.





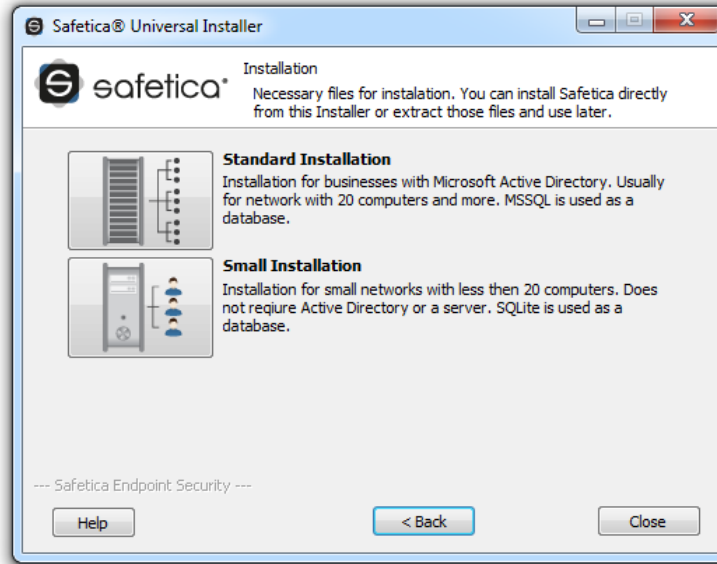
Safetica Management Service'in database'ler ile bağlantısı, Safetica Management Console üzerinde "Server settings" kısmından ayarlanır. Bu bağlantının nasıl yapılacağıyla ilgili tarif için bkz: [Safetica Management Service Yapılandırılması](#)

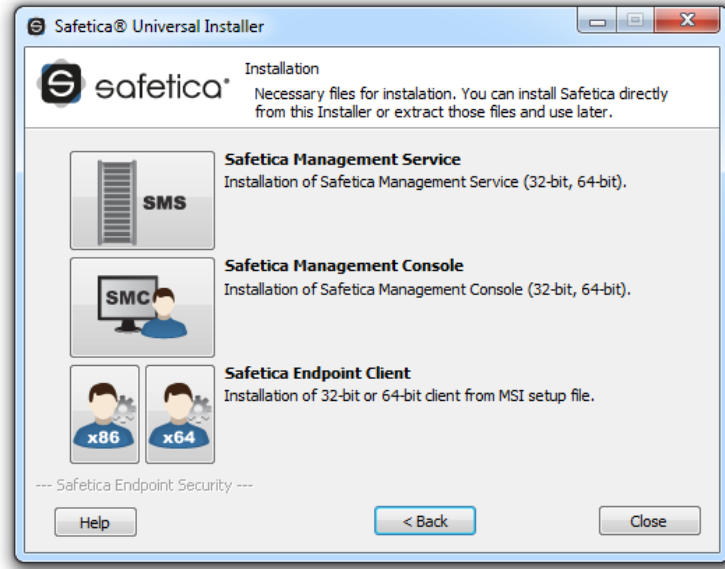
3.1.2 Safetica Management Service'in Kurulumu

Safetica Management Service Safetica'nın merkezi bir sunucu bileşenidir. Tüm Safetica client'larının (SEC), konsolun (SMC) ve database'lerin birbirleri ile bağlantılı olmasını sağlar. Standard kurulumda, merkezi database'leri için Microsoft SQL Server'ı kullanır. Safetica Management Service kurulmadan önce, içerisinde üç boş database ile Microsoft SQL Server kurulmuş olmalıdır.

Kurulum için aşağıdaki adımları izleyin

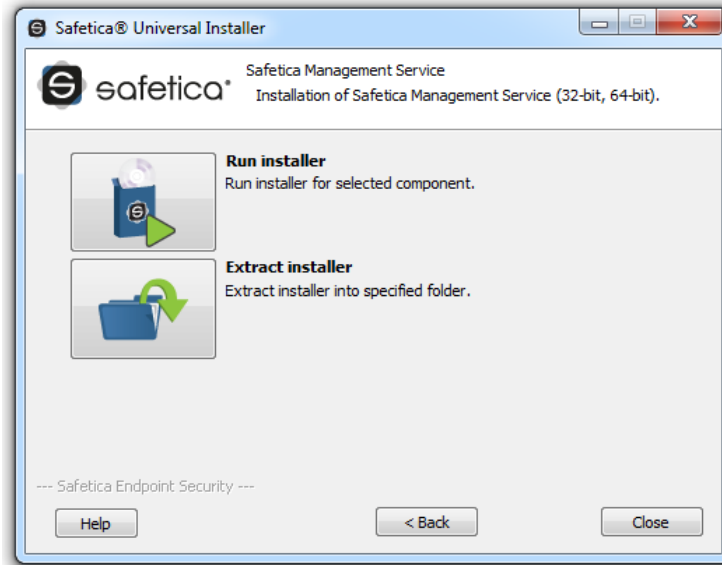
1. İndirdiğiniz kurulum paketini çalıştırın. Dilinizi seçtikten ve lisans koşullarını kabul ettikten sonra Installation -> Standard installation -> Safetica Management Service seçeneklerini izleyin.





2. Burada iki seçeneğiniz var.

- "Run Installer"a tıklayarak kurulumu direkt kurulum paketi üzerinden yapabilirsiniz.
- "Extract Installer"a tıklayarak daha sonra da kullanabileceğiniz Management Service kurulum dosyasını kaydedebilirsiniz.



3. İki seçenekten biri ile kurulumu çalıştırdıktan sonra, dilinizi bir kez daha seçerek lisans şartlarını kabul edin. Kurulum klasörünü seçin.
4. Kurulumdan önce "Integration settings"i (entegrasyon seçeneklerini) pasif yapabilirsiniz. Varsayılan modda bu seçenek aktiftir (tavsiye edilen).
5. Kurulumu tamamla. Safetico Management Service otomatik olarak kurulup başlayacaktır.
6. Kurulum başarıyla tamamlandıktan sonra, STAService.exe hizmetinin çalıştığından emin olun. (Görev yöneticisi -> Servisler (Hizmetler) -> STAService)
7. Son olarak, Firewall ve antivirüs yazılımınızda STASer-vice.exe işlemi ve 4438 ve 4441 portları için gerekli izinlerin tanımlı olduğundan emin olun.

Not: Varsayılan olarak, Safetico Management Console Safetico Management Service'ye bağlanmak için port 4441'i ve Safetico Endpoint Client'e bağlanmak için port 4438'i kullanır. Buralarda farklı portlar kullanmak için bu ayarları değiştirebilirsiniz.

3.1.3 Safetica Management Console Kurulumu

Konsol yazılımının yönetiminin merkezidir. Safetica Endpoint Client'ların (SEC) ve Safetica Management Services'in (SMS) ayarlanması ve yönetilmesi için olduğu gibi database yönetimi ve tabi ki Safetica modüllerinin yönetimi için de kullanılır. Konsol ayrıca istatistikleri, grafikleri ve izleme çıktılarını gösterir. Safetica Management Console'u (SMC) kullanarak birden fazla SMS örneğini yönetebilirsiniz. Tek ihtiyacınız olan SMC'nin yönetilen SMS'e erişimi olan herhangi bir bilgisayarda kurulu olmasıdır. Ne konsol kurulumlarının ne de bu konsolların kullanıcılarının sayısı lisans ile sınırlandırılmamıştır.

Kurulumu aşağıdaki gibi devam edin

1. Daha önce indirdiğiniz kurulum paketini açın. Dilinizi seçtikten ve lisans koşullarını kabul ettikten sonra, Installation -> Standard Installation -> Safetica Management Console adımlarını izleyin.
2. Burada iki seçeneğiniz var.
 - o *Run installer* buton'una tıklayarak kurulumu kurulum paketinden çalıştırın.
 - o "Extract Installer"ı seçerek, daha sonra kurabileceğiniz SMC kurulum dosyasını çıkartın.
3. İki seçenektan biri ile kurulumu çalıştırarak, bir kez daha dilinizi seçin ve lisans koşullarını kabul edin. Kurulum klasörünü seçerek kurulumu tamamlayın.
4. Son olarak firewall ve antivirüs yazılımlarınıda STCon- sole.exe işlemi için gerekli izinlerin tanımlandığından emin olun.

3.1.4 Safetica Management Service Yapılandırması

Safetica Management Console (SMC) ve Safetica Management Service'in (SMS) başarıyla kurulumundan sonra, kullanıcı bilgisayarlarında Safetica Endpoint Client'ların kurulumuna başlamadan önce sistemin tamamı doğru bir şekilde yapılandırılmış olmalıdır.

Baslıca yapılandırma adımları aşağıdaki gibidir:

1. SMC'yi çalıştırın ve konsol için yeni bir şifre belirleyin.
2. Management and settings -> *Server settings* kullanarak SMC'yi SMS'in ilgili sunucu bileşenine bağlayın. Bunun için varsayılan kullanıcı bilgileri olan "kullanıcı adı: safetica" ve "parola: safetica" kullanabilirsiniz.
3. Üç Microsoft SQL Server database'i için oturum açma bilgilerini girin. Bu database'lerin oluşturulması ve çalıştırılması, ayarlar penceresinde değişiklikleri kaydetmeniz ardından otomatik olarak gerçekleşecektir.
4. Tercihe bağlı olarak Active Directory senkronizasyonunu sağlayabilirsiniz. Bunu Management and settings -> *Server Settings* -> Active Directory kısmından uygun organizasyon birimini seçerek yapabilirsiniz. Bu organizasyon birimi altındaki kullanıcı ve bilgisayarlar Kullanıcı Ağacında ad grubunun altında gösterilecektir.
5. SMC'yi kullanarak kategori database'ini güncelleyin. Bunun için, Management and settings-> *Categories sekmesini kullanabilirsiniz.*
6. Varsayılan SMS hesabı için varsayılan şifreyi (safetica) değiştirin. Bunun için, *Management and settings -> Server Settings -> Change connected SMS user password menüsünü kullanabilirsiniz.* Uygun sunucuyu seçin ve şifrenizi değiştirin.
7. Safetica Endpoint Client'ın (SEC) yerel yönetimi için şifrenizi değiştirin- Önce olduğu gibi varsayılan şifre yine "safetica" dir.

8. Bir Lisans anahtarınız varsa *Management and settings* -> *License management* sekmesine bunu girebilirsiniz. Lisans yalnızca Safetica Endpoint Client'lara uygulanır. Safetica fonksiyonları client'a uygun modülün aktivasyonu yapıldığında aktif olacaktır. Bu işlem Client'ı kurup sunucuya bağladıktan sonra aynı menüden yapılabilir.

SMS ayarlamalarının detaylı tarifi:

1. Konsolu ilk çalıştırmamızda, açılan bir oturum açma penceresi yeni bir yerel şifre girmenizi isteyecektir. Bu parola yalnızca konsol erişiminizi korur. SMS bağlantınızla ilgisi yoktur. Yeni bir parola girin ve onaylayın.

SMC'yi her açtığınızda bu parola sorulacaktır. SMC parolası *Management and settings* -> *Console settings* sekmesinden değiştirilebilir.

2. Şimdi yeni SMS'e bağlanmanız gereklidir. *Management and settings* -> *Server settings* sekmesini açın. "New server"a tıklayın ve SMS'in çalıştığı bilgisayarın adresini domain formunda (server.com) ya da IP address olarak girin (Eğer kurulmuş birden fazla SMS varsa, bir tanesini girin). Ayrıca SMS ile haberleşilen portu da belirleyebilirsiniz. Bu port varsayılan olarak port 4441'dir. Bu portu "STASer-vice.exe -adminport <yeni port numarası>" komutunu Administrator olarak açtığınız cmd ekranından, SMS'in kurulum klasörün içerisinde girerek değiştirebilirsiniz. Değişiklik SMS servisi yenden başladığında aktif olacaktır.

Her SMS önceden tanımlanmış bir administration hesabı ile gelir. Aşağıdaki kullanıcı adı ve parola ile oturum açabilirsiniz:

Username: safetica

Password: safetica

Bunları uygun alanlara girin. SMS'e bağlandıktan ve SMC'yi çalıştırdıktan sonra, parolayı değiştirmenizi öneririz. Bu işlemi *Management and settings*-> *Server settings* -> *Change connected SMS user password* menüsünden yapabilirsiniz.

Safetica Management Console

Overview Console settings **Server settings** Categories Zones Database management Update Synchronization Access Management SMS access log Settings Overview Templates Client settings

Clients Information Integration settings License management

Server settings

BASIC INFORMATION << Hide

Using the server settings you can set connections to one or more SMS you want to manage. Each SMS can have its own database connection, AD synchronization and SMTP server for sending e-mails. You can also change the password for currently connected user. Help

CONNECTION TO SAFETICA MANAGEMENT SERVICE << Hide

New server Edit Remove

Service	Username
192.168.29.135	safetica

Version and name << Hide

Version: 5.0.0

Server Name: SMS The name of the server provides a unique server identification throughout Safetica

Databases connection settings << Hide

Database: Main database Test connection

Server: 192.168.29.135 Enter a server address reachable from all client computers.

Port: 1433

Database name: ses5_main_RC

Username: sa

Password: ●●●●●●

Safetica Data Calculator: <http://calc.safetica.com/>

ACTIVE DIRECTORY << Hide

Add Remove

Connected nodes:

- Giriş bilgisini onayladıktan sonra SMC, SMS'e bağlanır. Bir bağlantı kurulduğunda, SMS sertifikası içeren bir pencere belirir. "Yes" diyerek geçebilirsiniz.
 - Sıradaki aşamada bir üç database'e bir MS SQL database bağlantısı kurun. Management and settings -> Server settings -> Databases connection settings menüsünde açılır menüden bir database seçin ve hepsi için uygun ayarları girin:
 - Server – MS SQL örneğini çalıştıran sunucunun domain formunda ya da IP adresi olarak adresi. SQL örneğini zaten isimlendirdiyse, adresi "server adresi\MS SQL örneğinin adı" şeklinde girin (örn. 192.168.10.1\SQLinstance).
 - Port – MS SQL örneğinin üzerinden haberleştiği portun numarası (Standart port 1433'tür).
 - Database name – oluşturacağınız database'in adı. Database otomatik olarak oluşturulur.
 - Username – yukarıda bahsedilen database'lerin yönetimine ve database oluşturmaya yetkili MS SQL database kullanıcısının adı.
- Not:* MS SQL server kullanıcıları "authentication mode"u, (SQL Server Authentication) ya da (mixed mode) olarak ayarlamalıdır. MS SQL örneği de ayrıca bu oturum açma metodunu desteklemelidir.
- Password - database kullanıcısının parolası.

Girilen verinin doğruluğunu ve Safetica Management Service ile MS SQL fonksiyonları arasındaki bağlantıyı "Test connection" butonuna basarak test edebilir.

Sayfanın altındaki "Add" butonu ile Active Directory köklerini SMS yönetimine aktarabilirsiniz. Bir onay penceresinin ardından, bu rootlardan tüm domain kullanıcı ve bilgisayarları kullanıcı ağacına eklenecektir (Ayarladığınız SMS üzerine). Bunlar başlangıçta ActiveDirectory için ayrılan (AD) kısmına alınır ve isterseniz bunları sonradan yeni oluşturacağınız gruplara aktarabilirsiniz. Daha fazla bilgi için "görselleştirme ve ayar modları" kısmına bakın.

Database'lerdeki veri boyutları

İzleme sırasında biriken verinin boyutu direkt olarak kullanıcı sayısı ve bu kullanıcılar için tanımladığınız aktif izleme modülleriyle orantılıdır. Veri hesaplayıcımızı kullanarak bu değişkenlere bağlı yaklaşık bir veri boyutu hesabı edebilirsiniz. Hesaplayıcımızı <http://calc.safetica.com/> adresinde bulabilirsiniz.

5. Firma ağınıza birden fazla SMS kurduysanız, yukarıda bahsedilen basamakları diğer SMS'ler için de uygulamanızı tavsiye ederiz. Bir başka SMS için sunucu ayarlarını görüntüleyin; bunu konsolda Management and settings -> Console settings sekmesinden yapabilirsiniz. "New server" butonuna tıklayın ve bağlantı bilgisini girin. Tüm SMS'ler için konsolu kullanın. Öncelikle, varsayılan yönetici hesabının şifresini değiştirin. Daha sonra Management and settings -> Access management sekmesinden her SMS için istediğiniz erişim hakları ile erişim hesapları oluşturun. Her SMS kendi özel erişim hesaplarına sahiptir. Muhtemel erişim hesapları ve bunların yetkileri için örnekler:

Güvenlik Yöneticisi – DLP ve Supervisor modül ayarlarına erişebilir. Çalışanların izlenmesiyle edinilen hiç bir datayı göremez.

Müdür – tüm modüllerden gelen görüntüleme verisine erişebilir ancak hiç bir ayarı değiştiremez.

Denetleyici – Auditor modülünün ayarlarını değiştirebilir ve çalışanların izlenmesi ile edinilen verileri görüntüleyebilir.

Tabi ki her SMS için oluşturduğunuz kullanıcıların haklarını dilediğiniz gibi düzenleyebilirsiniz. Hesap ayarları ve her modül için erişim hakları düzenleme için Access management kısmına bakınız.

6. Şimdi güncel bir kategori database'i indirmeniz gerekmektedir. SMC'nin ana menüsünden "Management and settings -> Categories -> Update"e gidin. Aşağıdaki üç seçeneği içeren bir pencere açılacak:

1. İnternette güncelleme (service'e) – database güncelleme SMS sunucu service'i tarafından yapılır. Güncelleme esnasında ilerlemeyi gösteren bir pencere açılır.

Not: Bu seçenek için Safetica Management Service'in internet erişimi olmalıdır.

2. Klasörden güncelleme (service'e) – database güncelleme harddisk üzerinde bir güncelleme klasöründen yapılır. Bu metod internet erişiminiz olmadığında ve indirilmiş güncelleme dosyası bulunduğunda uygundur. Girmeniz gereken yol, SMS çalıştıran bilgisayar üzerindeki güncelleme dosyasının yoludur. SMC Konsolunu çalıştırdığınız bilgisayar üzerinde bir yol değildir.

3. Güncellemeleri indirme (konsola) – Güncelleme dosyası web sunucusundan bilgisayarınıza indirilir. Dosyayı sunucu servisine elle ya da yukarıda bahsedilen "klasörden güncelleme" yoluyla yüklenebilir. İlerlemeyi gösteren bir pencere açılacaktır.

Kurulumun bu aşaması şart değildir ancak kategoriler bu güncelleme yapıldıkça kadar aktif olmayacaktır.

7. Son olarak da kullanıcılara modül lisanslarını atamanız gerekmektedir. Bunu Management and settings -> License Manager altından SMC.

License Manager'a anahtarınızı girin ve onayladıktan sonra, orta kısımda kullanıma müsait lisansların sayısını göreceksiniz. Daha sonra lisansları gruplara, kullara ya da kullanıcılara atayabilirsiniz. Bu şekilde hangi grup ya da kol tarafından ne kadar lisans kullanılabileceğini kontrol altına almış olursunuz. Yeni bir SEC'i SMS'e (database) bağladığınızda, atanmış olan lisans istemciye indirilecek ve License Manager'daki boş lisans adedi buna bağlı olarak azalacaktır. Lisans yönetimi hakkında daha fazla bilgiyi License Manager kısmından edinebilirsiniz.

Ayrıca, *Safetica Endpoint Client*'in kaldırılması, güncellenmesi ya da kapatılması için parolalarınızı değiştirmenizi şiddetle tavsiye ediyoruz. Bunu, *Management and settings* -> Client settings sekmesindeki Allowed actions kısmından yapabilirsiniz. Daha fazla bilgi için *Safetica Endpoint Client Protection*' a bakınız.

3.1.5 Safetica Endpoint Client kurulumu

Safetica Endpoint Client (SEC) Safetica'nın kurulacak son bileşenidir. Client makinalarda güvenlik ilkelerinin uygulanmasını ve Safetica Management Console (SMC) üzerinde yapılandırılmış olan ayarların bu makinalar üzerinde düzgün çalışmasını sağlayan esas bir bileşendir. Son kullanıcılar için, ayrıca bir dizi güvenlik aracı sağlar.

Kuruluma aşağıdaki gibi devam edin:

1. İndirmiş olduğunuz kurulum paketini açın. Dilinizi seçerek lisans koşullarını kabul ettikten sonra, *Installation > Standard Installation> Safetica Management Client x86* ya da *x64* kısmından devam edin – bu son kullanıcıda kurulu olan işletim sistemi versiyonuna göre değişir.
2. Burada iki seçeneğiniz var.
 - o Setup'ı direkt olarak kurulum paketinden çalıştırın, "Run installer" butonu.
 - o Yalnızca SEC installer'ı çıkartın, bunu daha sonra kurulum için kullanabilirsiniz.
3. Kurulumu çalıştırmadan önce sizden aşağıdaki detaylar istenecek:
 - o *Server adresleri* – SEC'in bağlanacağı SMS'in adresi.
 - o *Port* – SMS'in dinlediği port. Varsayılanı 4438'tür.
 - o *Language of client* – SEC'in dili.
 - o *Hidden safetica processes* – Tüm SEC işlemleri bu seçenek işaretlendiğinde kurulumdan hemen sonra gizlenir. (*STCService.exe, STPCLock.exe, STMMonitor.exe, STUser-App.exe, and Safetica.exe*). Bu Management and settings -> Client settings -> Hide safetica processes 'den değiştirilebilir.
 - o *Client mode* – Endpoint Security Tools'un grafik arayüz modu. Bu, *DLP -> Endpoint Security Tools settings -> Client GUI mode 'dan değiştirilebilir.*
4. Kurulumu çalıştırdıktan sonra (kurulum paketinden ya da dışarı çıkarttığımız yerden), dilinizi bir kez daha seçerek lisans koşullarını kabul edin.
5. Kurulum klasörünü seçin.
6. Kurulumu tamamladıktan sonra, STCService.exe servisinin çalıştığından (Windows Görev Yöneticisi > Servisler > STCService – çalışıyor) emin olun.
7. Son olarak güvenlik duvarınızda ve anti-virüs yazılımınızda şunlar için izinler tanımlayın: STCService.exe, STPCLock.exe, STMMonitor.exe, STUserApp.exe, ve Safetica.exe.

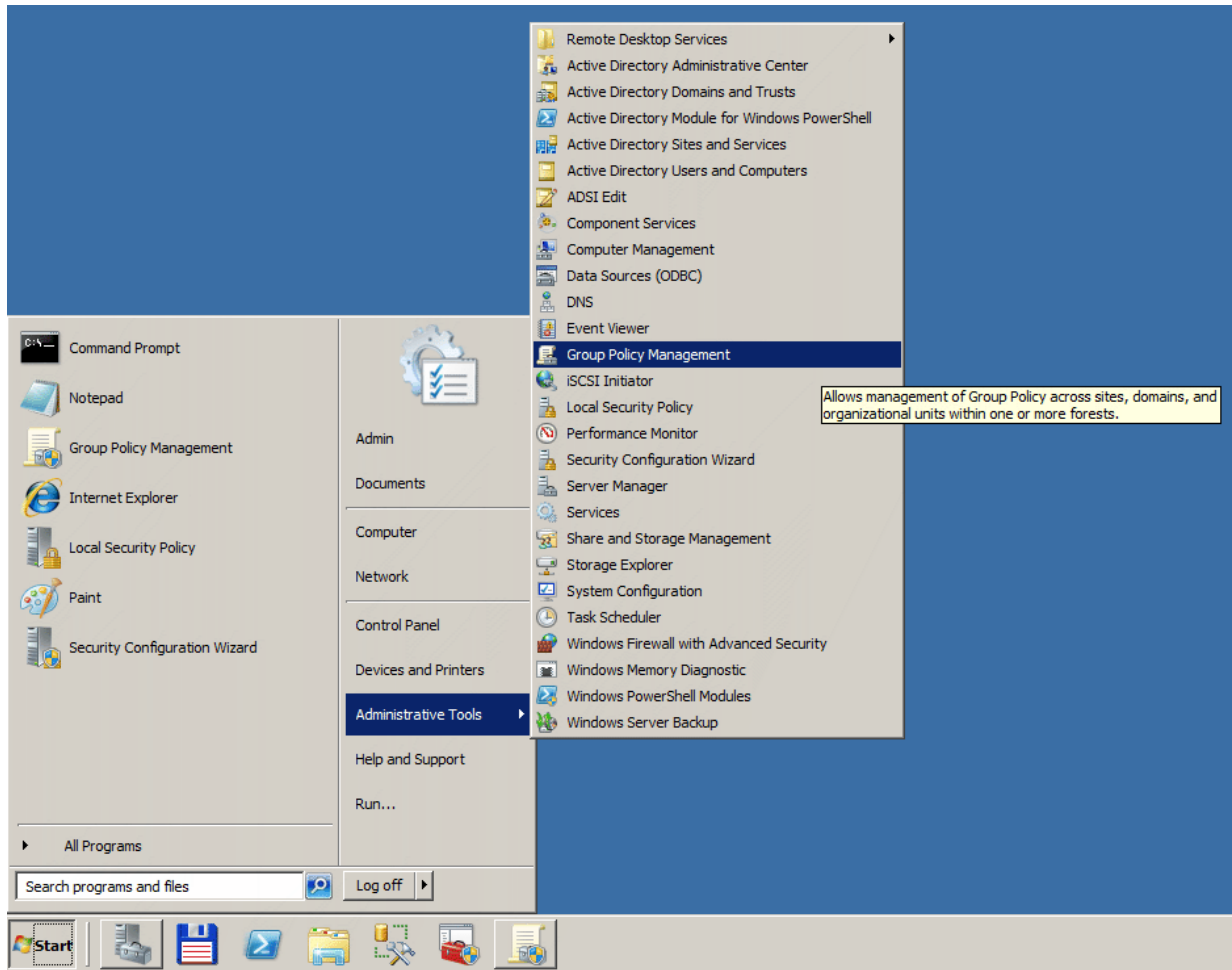
SEC'i yapılandırmak için, Safetica ürününün geneli için olduğu gibi, [After Installation](#) kısmını okuyarak devam edin.

3.1.5.1 GPO kullanımı ile kurulum

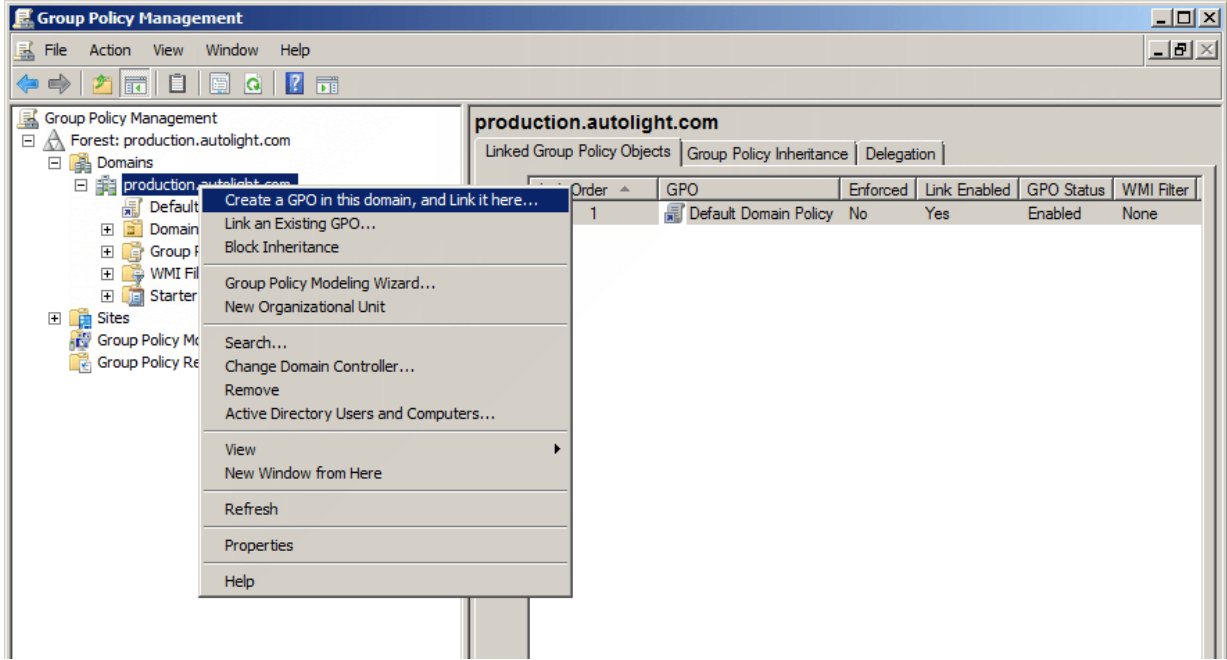
Safetica Endpoint Client'ların, Group Policy Management kullanımı ile toplu kurulumu da mümkündür. Bunu yapmadan önce, Safetica Endpoint Client'ın MSI paketini Safetica kurulum paketinden çıkartmalısınız.

Burada kurulumun yalnızca bir yolunu anlatacağız – assign (buradaki tarif gerçeğe her zaman uymayabilir; işletim sisteminize göre menü adları değişebilir). Aşağıda Windows Server 2008 R2 üzerinde GOP kullanımı ile toplu kurulum anlatılmıştır:

1. Safetica kurulum paketini açın.
2. *Standard installation'ı seçin.*
3. İlgili kullanıcı işletim sistemine göre kurulum türünü seçin (x86 ya da x64)
4. MSI paketini bir paylaşımlı diske ya da klasöre çıkartın ve bu klasöre erişim haklarını düzenleyin (açma ve okuma hakları yeterli olacaktır). Bu haklar arzu edilen kullanıcı grupları için bağlayıcı olacaktır (varsayılan olarak bu grup *Domain Users* ve *Domain Computers* olacaktır).
5. SEC kurduğunuz sunucuya GPO ile uzaktan erişin. *ManagementTools* -> *Management of group policies kısmını açın.*

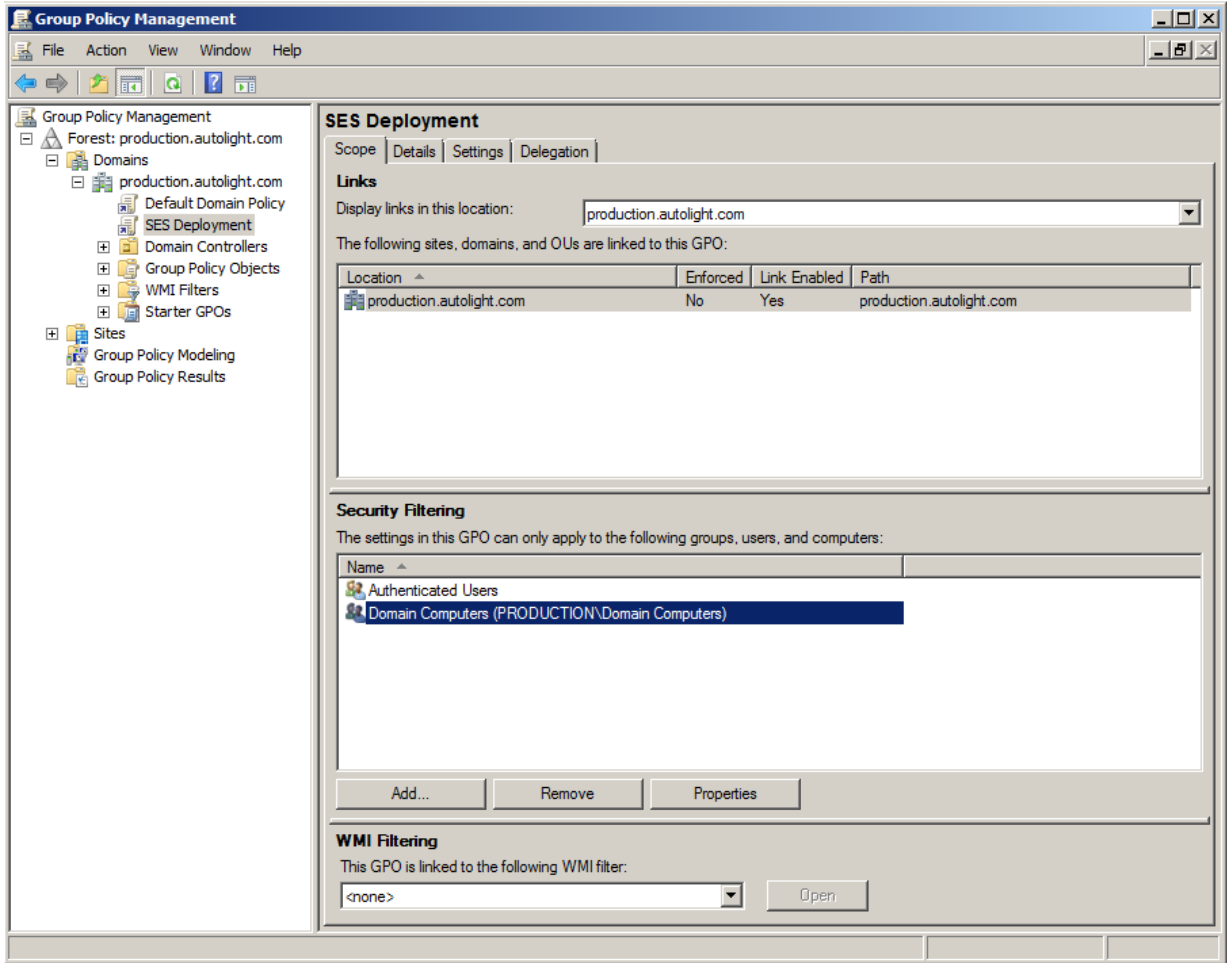


6. SES kurmak istediğiniz organizasyon birimi üzerine sağ tıklayın ve "Create new group policies object in this domain and interconnect it..." menüsünü seçin.

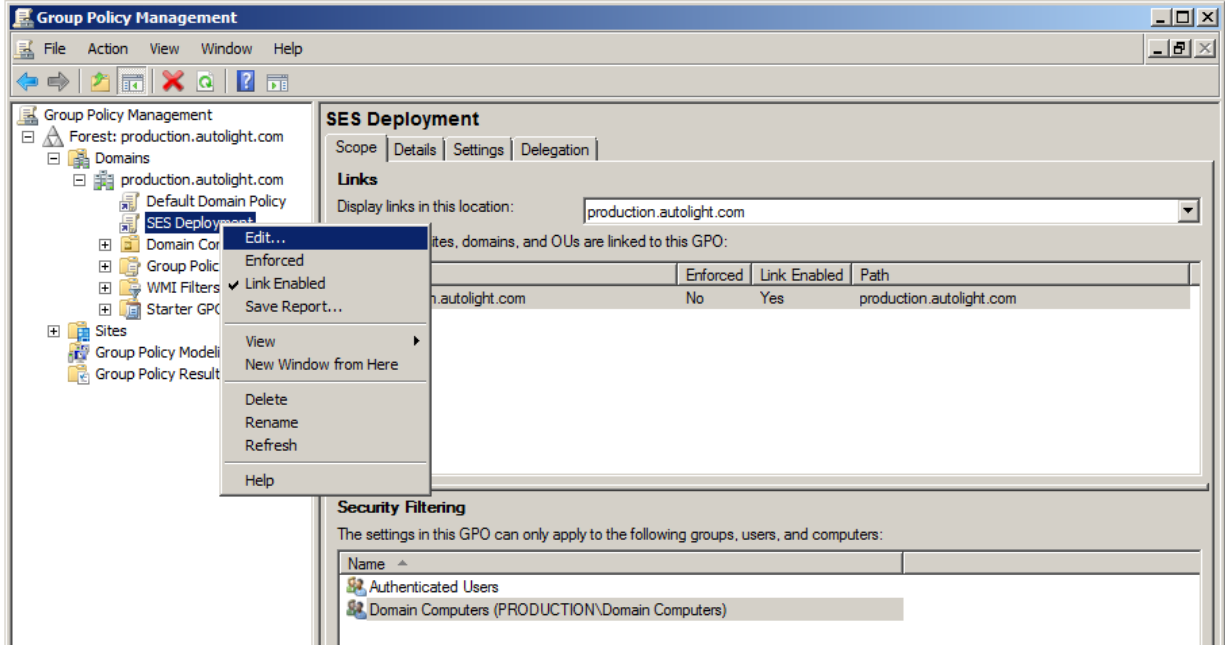


7. Yeni projeye bir isim verin (örn. SES Deployment).

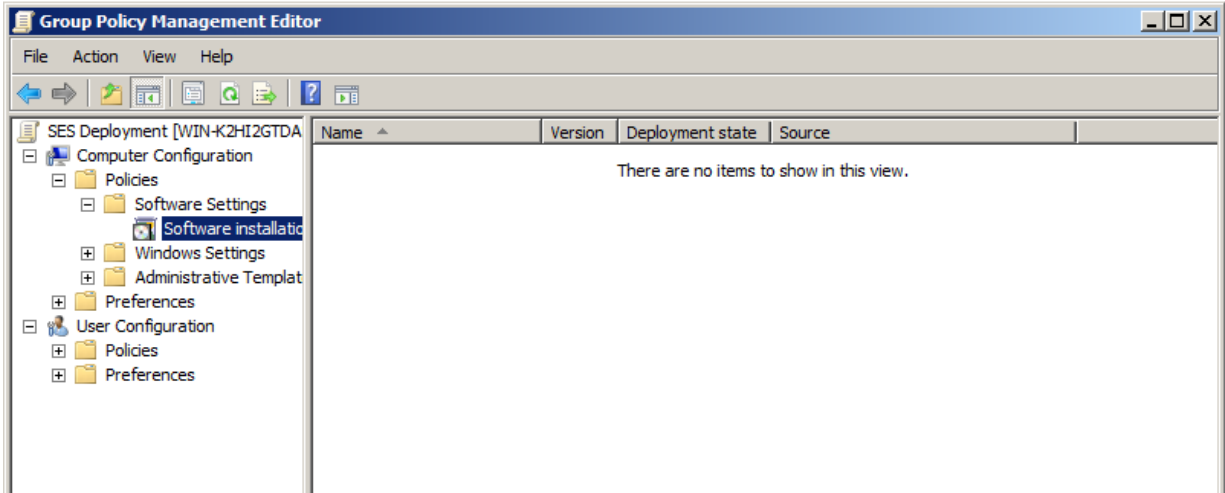
8. Pencerenin sağ kısmından yeni öğeyi seçin ve Domain Computers grubunu zaten var olan Authenticated Users'a ekleyin.



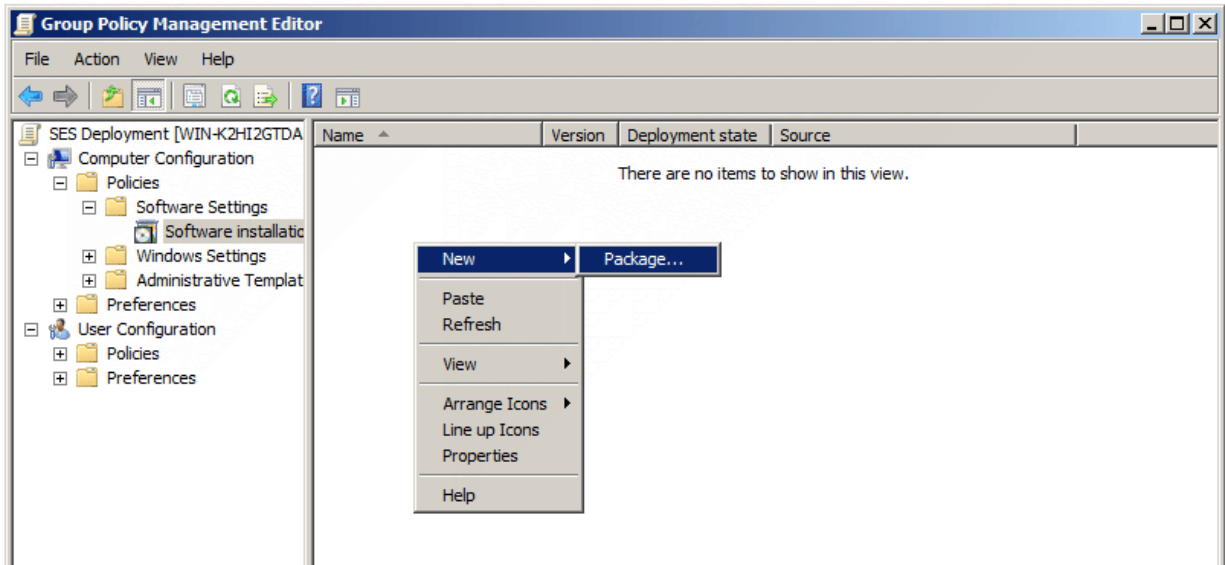
9. Yeni oluşturulan grup ilkenizi seçin ve sağ tıklayarak *Edit'i* seçin.



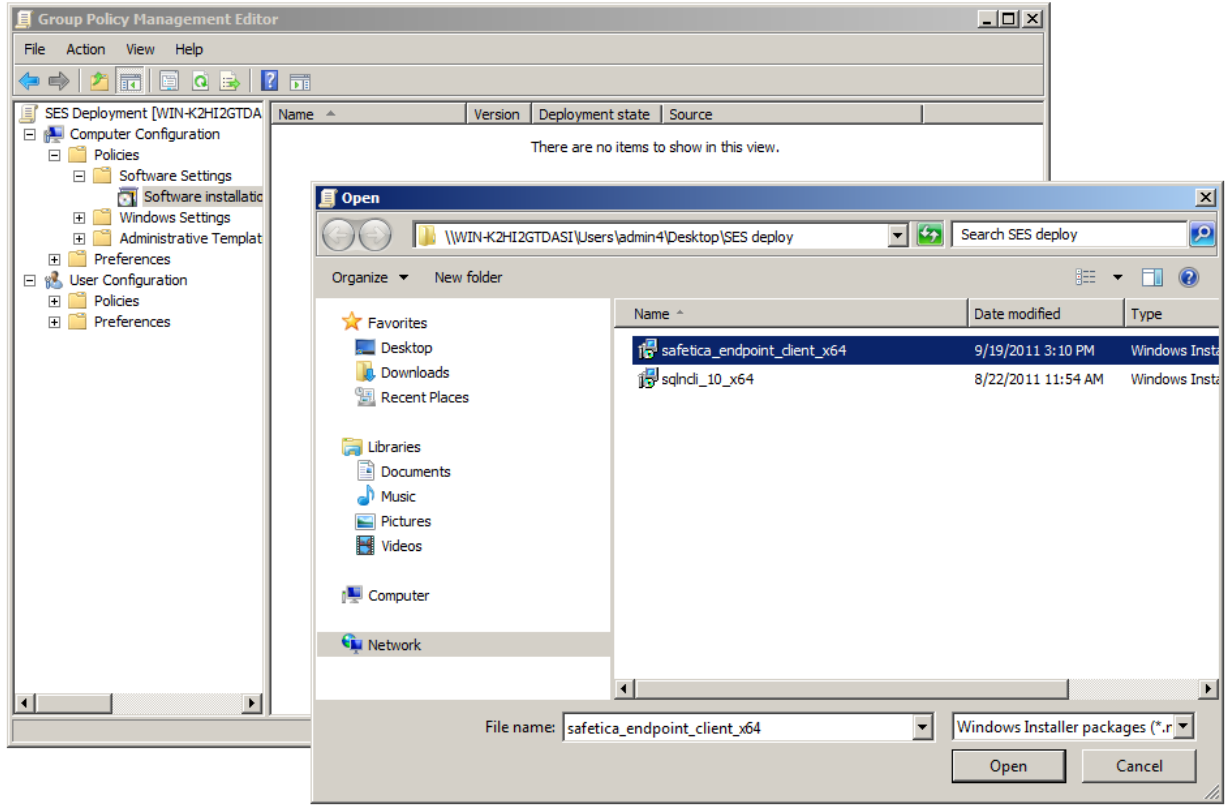
10. Açılan pencerede *Computer setup* -> *Policies* -> *Software settings*'i seçin ve *Software installation* 'a tıklayın.



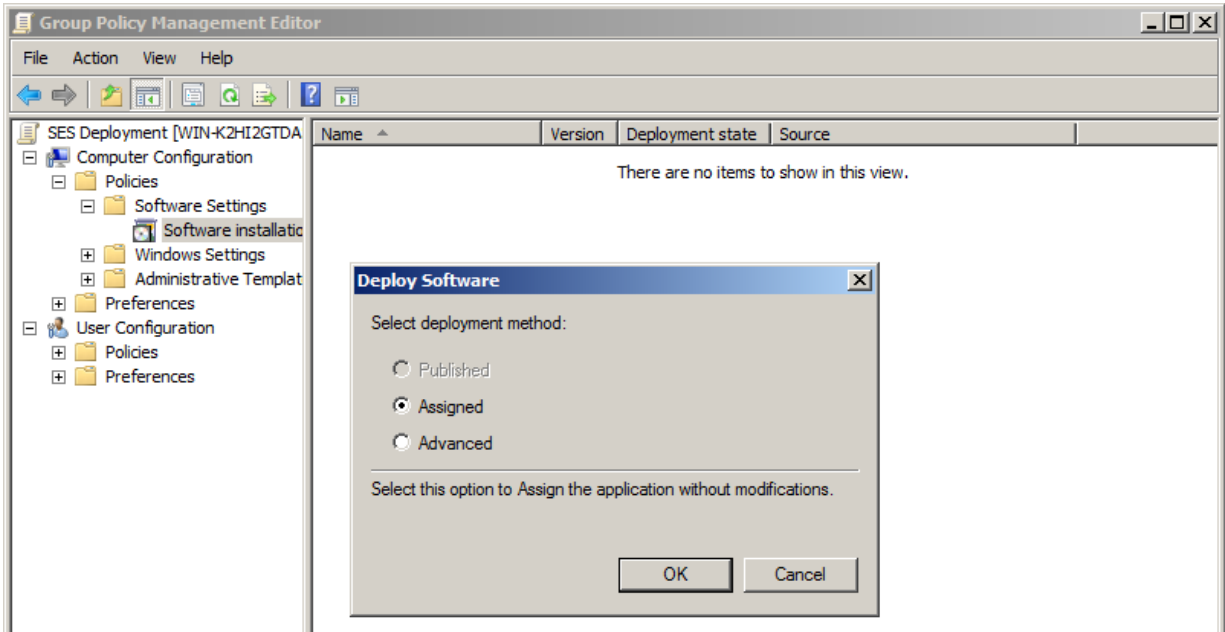
11. Orta ekranda sağ tıklayın ve *New item* -> *Package...* 'ı seçin.



12. MSI paketinin iletişim penceresinde içerisine MSI paketini ve SEC'i kopyaladığınız paylaşım dosyalarını seçin ve daha sonra paketi seçin.

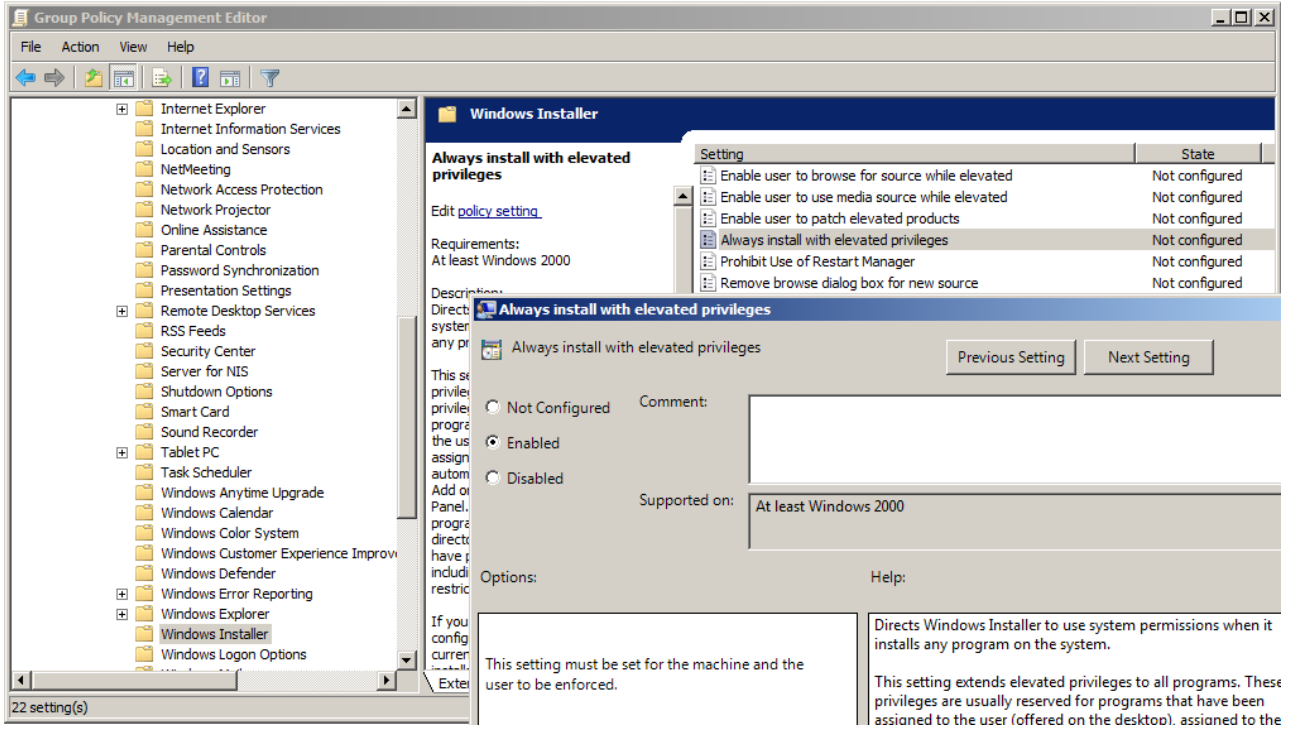


13. Sıradaki iletişim penceresinde Assigned'ı seçin ve onaylayın.

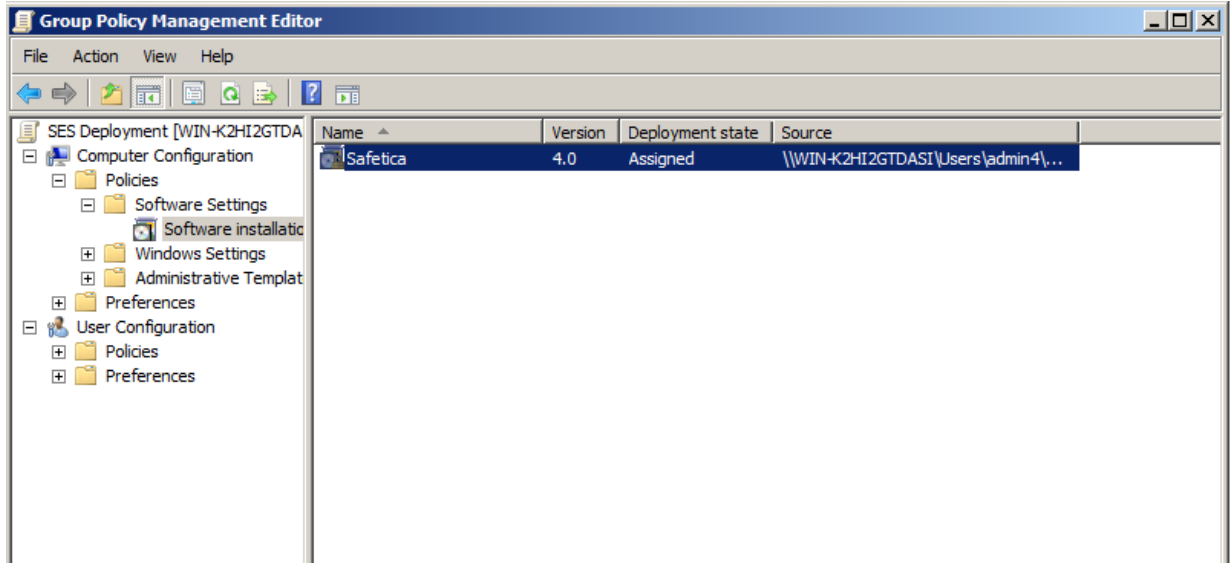


Uyarı! 32-bit MSI paketinden kurulum yaparken, 64-bit sistemlere kurulumun engellenmesi gerekir. Bunu Advanced -> Deployment -> Extended -> Specify -> içerisinde yayıllım metodunu seçip "Make this 32bit version of X86 application available for computers with the Win64 architecture" seçeneğindeki işareti kaldırarak yapabilirsiniz.

14. Ardından *Computer setup -> Management templates -> Windows components -> Windows Installer*'ı açın. Burada "Always install with elevated privileges" ögesini göreceksiniz. Bunu *Enabled* yapın. Böylelikle Safetica Endpoint Client 'ın kullanıcılara sorunsuz kurulumundan emin olacaksınız.



15. İlgili bilgisayarlar yeniden başlatıldıktan sonra, SEC otomatik olarak kurulmaya başlayacaktır.



16. İlke yapılandırması tamamlanmıştır ve dağıtıma hazırdır. Safetica Endpoint Client kullanıcı bilgisayarı yeniden başladığında otomatik olarak başlayacaktır.

Safetica'nın yapılandırılması ve ayarlanması için [After installation](#) kısmına geçin.

3.1.6 Kurulumdan sonra

Tüm Safetica bileşenlerini kurduktan sonra, Safetica'yı kullanmaya başlamadan önce yapmanız gereken son birkaç dokunuş kaldı.

1. Öncelikle tüm Safetica Endpoint Client'larının (SEC) sunucuya bağlandığından emin olun - Safetica Management Server (SMS)-. Kullanıcı ağacında, kullanıcılar ve bilgisayarlar renklerle ifade edilir.

- John-PC
- John SEC online ve SMS'e bağlı.

- John
John-PC SEC offline ve SMS'e bağlı değil.

- İstemcilere ilgili modülleri atamak için License Manager'ı kullanın. Kendisine lisans atanan her bilgisayar ve modül bir "tik" ile gösterilecektir. Atanmış lisanslar olmaksızın, modül özellikleri aktif olmayacaktır.

Safetica Management Console

Overview Console settings Server settings Categories Zones Database management Update Synchronization Access Management SMS access log Settings Overview Templates Client settings

License management

BASIC INFORMATION

You can use the License manager view to assign the licenses for all Safetica modules. Licenses are then assigned to endpoints.

LICENCE SETTINGS

Insert new licence key All periods

General Advanced

Modules	Available	Total	Details
Auditor	0	100	100 (2013.02.06 - 2013.04.06)
Supervisor	0	100	100 (2013.02.06 - 2013.04.06)
DLP	0	100	100 (2013.02.06 - 2013.04.06)

Users and groups

	Auditor (activated / available)	Supervisor (activated / available)	DLP (activated / available)
SMS	11 / 89	11 / 89	11 / 89
Unknown			
Active Directory			
FT-XP			
HB			
jan			
PC-JB	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MP			
TJango			
PU			
JŞ			
VS			
PU-jap			
Business			

- DLP modülüne bir lisans atadıysanız, Client GUI mode'unu seçin. Varsayılan olarak, çalışanlarınız Endpoint Security Tools özelliklerine erişebilir (Normal mode). Üç mod arasından seçim yapabilirsiniz (DLP -> Endpoint Security Tools settings -> Client GUI mode):
 - *Normal* – güvenlik araçları ve içerik menüsü içeren bir Endpoint Security Tools kullanıcı arayüzü.
 - *Tray only* – kullanıcılar yalnızca içerik menüsünden erişilebilen temel fonksiyonlara ulaşabilir. Kullanıcı arayüzü yok.
 - *Invisible* – kullanıcılar ne içerik menüsüne ne de Endpoint Security Tools fonksiyonlarına erişebilir.

EST settings

BASIC INFORMATION << Hide

Endpoint Security Tools (EST) are part of Safetica Endpoint Client and are available only when there is a valid Safetica DLP licence. The user can utilize EST to manage the encrypted disks, use the data shredder or the password database. In the following sections you can set basic security settings for EST at endpoint to force the appropriate security level.

SYSTEM SETTINGS

Run on system startup: Inherit

Associate .dco, .dcf and .dcd files with Safetica: Inherit

DISK AND ENVIRONMENT SETTINGS

Client GUI mode: Inherit

Forced disk unmounting: Inherit

Access to connected disks: Inherit

Forced disk unmounting hotkey (Win-Ctrl-Q): Inherit

Disk unmounting hotkey (Win-Ctrl-U): Inherit

SECURITY RULES

Data shredder mode: Inherit

Forced disk password change: Inherit

Change password every: days

Passwords remembering: Inherit

Minimum password level: Inherit

Enforce these settings on client: Inherit

4. Düzgün veri aldığınızdan emin olabilmek için bazı fonksiyonları etkinleştirmeyi deneyin (örn. *Application monitoring*)

Bu noktada, Safetica kullanıma hazırdır.

3.2 Küçük kurulum

Safetica'nın küçük kurulumu az sayıda bilgisayar içeren ağlar için tasarlanmıştır (20 ya da daha az bilgisayar). Kurulum Microsoft Active Directory'i desteklemez ve bir sunucu işletim sistemine ihtiyaç duymaz. Ana database'ler için Safetica Management Service (SMS) kurulduğunda otomatik olarak kurulacak ve yapılandırılacak olan SQLite database kullanılır, böylelikle başka bir yapılanmaya gerek duymaz. SQLite Safetica Management Service'in bir yapılanma içerisindeki birden fazla örneğini çalıştırabilir.

Küçük kurulum yapılırken aşağıdaki basamakları izleyebilirsiniz:

1. Kurulumu başlatmadan önce, ağınızın belirtilen servis gereksinimleri'ni karşıladığından emin olun.
2. Dilediğiniz bilgisayarlara [Safetica Management Service'i kurun](#). Ayarlara ve kayıtlara ait merkezi veri tabanları otomatik olarak aynı bilgisayarlar üzerine kurulacaktır.
3. Safetica'yı yönetmek istediğiniz bilgisayara [Safetica Management Console'u kurun](#).
4. Safetica Management Console'u kullanarak, Safetica Management Service'e bağlanın ve [sunucuyu yapılandırın](#).
5. Her bir istemci üzerine [Safetica Endpoint Client'ı kurun](#).
6. [Başlangıç kurulumunu yapın](#) ve tüm bileşenlerin doğru çalıştığından ve birbirleriyle haberleşebildiğinden emin olun.

Tüm bileşenleri kurarak kontrollerini yaptıktan sonra, Safetica'yı kullanmaya başlayabilirsiniz.

3.2.1 Kurulumdan Önce

Asıl kurulumdan önce aşağıdaki adımları uygulamaya dikkat edin:

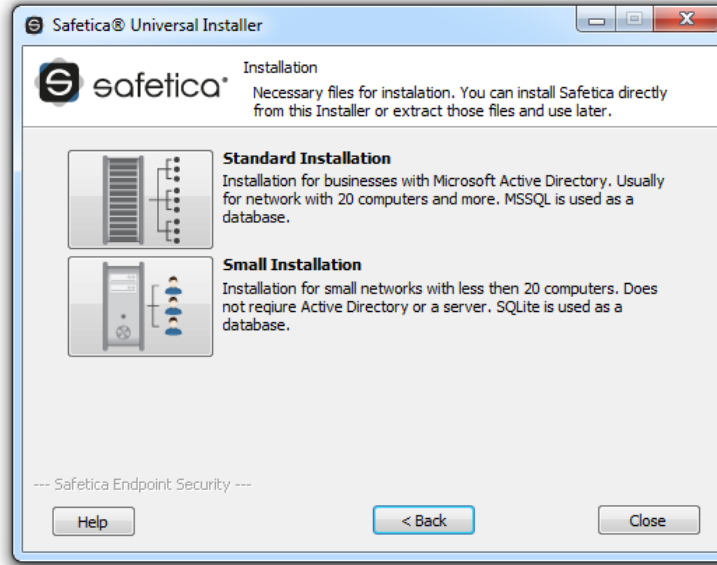
1. Safetika'nın her üç bileşeni için de donanım ve yazılım gereksinimleri 'nin karşılandığından emin olun.
2. İş ağınızın bir ön analizini yapın:
 - o Ağınızdaki hangi bilgisayarlar üzerinde Safetica Management Service'i (SMS), Safetica Management Console'u (SMC) ve Safetica Endpoint Client'ı (SEC) çalıştırmak istediğinize sırasıyla karar verin.
 - o Tüm bileşenleri aynı ağ üzerindeki bilgisayarlara kurduğunuzdan ve bunların karşılıklı olarak birbirlerine erişebildiklerinden emin olun.
3. Güvenlik duvarınıza ve anti-virüs yazılımınıza izinler tanımlayın:
 - o Safetica Management Service kurulumu yapacağınız bilgisayarlar üzerinde, STAService.exe işlemi ve şu portlar için izinler tanımlayın:
 - 4438 (SEC -> SMS iletişimi).
 - 4441 (SMC -> SMS iletişimi).
 - o SMC kuracağınız bilgisayarlarda, STACon-sole.exe işlemi için izinler tanımlayın.
 - o SEC kuracağınız bilgisayarlar üzerine, şu işlemler için izinler tanımlayın: STCSERVICE.exe, STMonitor.exe, STUserApp.exe, Safetica.exe, STPCLock.exe.
4. Safetica Security'nin son versiyonunu içeren kurulum paketini indirin.
 - o Kurulum paketi küçük kurulum için gerekli tüm bileşenleri içerir.

3.2.2 Safetica Management Service kurulumu

Safetica Management Service (SMS) Safetika'nın merkezi bir sunucu bileşenidir. Tüm Safetica Endpoint Client'larının (SEC) ve Safetica Management Console'un (SMC) birbirlerine bağlı olmasını sağlar. Küçük kurulumda, merkezi database'ler için SQLite kullanılır. Database'ler, SMS kurulumu ile otomatik olarak kurulur ve yapılandırılır. SQLite loglar, ayarlar ve kategoriler için merkezi bir veri tabanı görevi üstlenir.

Kurulumu devam etmek için aşağıdaki adımları izleyin:

1. İndirdiğiniz kurulum paketini açın. Dilinizi seçip lisans koşullarını kabul ettikten sonra, *Installation -> Small installation -> Safetica Management Service* yollarını izleyin.



2. Burada iki seçeneğiniz var:

- "Run Installer" a tıklayarak kurulumu direkt olarak kurulum paketinden çalıştırın
- Sadece SMS installer'ı daha sonra da kullanabilecek şekilde çıkartın. (Extract)



3. Kurulumu çalıştırdıktan sonra (kurulum paketinden ya da çıkarttığınız konumdan), bir kez daha dilinizi seçerek lisans koşullarını kabul edin. Kurulum klasörünü belirtin.
4. Kurulumdan önce halen "Integration settings"i pasif edebilirsiniz. Bu seçenek varsayılan olarak etkinleştirilmiştir (önerilen).
5. Kurulumu tamamlayın. Safetica Management Service otomatik olarak kurulup çalışacaktır.
6. Kurulum tamamlandığında, STAService.exe 'nin çalıştığından emin olun (*Windows Görev Yöneticisi > Servisler > STAService – çalışıyor*)
7. Son olarak, STAService.exe işlemi ve 4438 ve 4441 portları için güvenlik duvarı ve anti-virüs yazılımınızda gerekli izinleri tanımlayın.

Not: Varsayılan olarak, SMC port 4441'i SMS'e bağlanmak için ve port 4438'i SEC'e bağlanmak için kullanır. Farklı portlar kullanmak için bu ayarları da değiştirebilirsiniz.

3.2.3 Safetica Management Console kurulumu

Konsol yazılımının yönetimi için merkez noktadır. Burası hem Safetica Endpoint Client'ların (SEC) ve Safetica Management Service'lerin (SMS) hem de Safetica modüllerinin ayarlanması ve yönetimi için kullanılır. Konsol ayrıca istatistikleri, grafikleri ve izleme çıktılarını gösterir. Safetica Management Console (SMC) üzerinden, çoklu SMS örneklerini yönetebilirsiniz. Tek ihtiyacınız olan SMC'nin yönetilen SMS'e erişebilen bir bilgisayarda kurulu olmasıdır. Ne kurulacak konsolların de de bunların kullanıcılarının sayısı lisansla sınırlıdır.

Kurulumu aşağıdaki gibi devam edin:

1. İndirdiğiniz kurulum paketini açın. Dilinizi seçerek lisans koşullarını kabul ettikten sonra, *Installation -> Small Installation -> Safetica Management Console* yolunu izleyin.
2. Burada iki seçeneğiniz var:
 - o "Run installer" butonuna tıklayarak kurulumu direkt kurulum paketinden çalıştırın.
 - o Yalnızca SMC installer'ı, daha sonra kullanmak üzere çıkartın (extract).
3. Kurulumu çalıştırdıktan sonra (kurulum paketinden ya da dışarı çıkarttığımız yerden), dilinizi bir kez daha seçerek lisans koşullarını kabul edin. Kurulum klasörünü seçerek kurulumu tamamlayın.
4. Son olarak *STCon-sole.exe* işemi için güvenlik duvarınızda ve anti-virüs yazılımınızda gerekli izinleri tanımlayın.

3.2.4 Safetica Management Service'in yapılandırılması

Safetica Management Console (SMC) ve Safetica Management Service'i (SMS) kurduktan sonra, kullanıcı bilgisayarlarında Safetica Endpoint Client 'ların (SEC) kurulumuna geçmeden önce tüm sistem doğru bir şekilde yapılandırılmalıdır. Tüm yönetim ve ayarlar SMC üzerinden yapılır.

Ana yapılandırma basamakları aşağıdaki gibidir:

1. SMC'e bağlanın ve konsol için yeni bir erişim parolası girin.
2. SMC'yi ilgili SMS'e varsayılan kimlik doğrulamasıyla *Management and settings -> Server settings* üzerinden bağlayın – login name: *safetica* ve password: *safetica*.
3. Kategori veri tabanını güncellemek için SMC'yi kullanın. Bunun için, *Management and settings -> Categories* sekmesini kullanabilirsiniz.
4. Varsayılan SMS hesabı (*safetica*) için varsayılan şifreyi değiştirin. Bunun için, *Management and settings -> Server Settings -> Password settings* menüsüne ulaşın. Uygun sunucuyu seçin ve parolanızı değiştirin (Bu işlem için sunucuda safetica hesabınız ile oturum açmış olmalısınız).
5. Safetica Endpoint Client 'ın (SEC) yerel yönetimi için parolanızı değiştirin– bkz. Safetica Endpoint Client'ına yetkisiz müdahale. Önce olduğu gibi, varsayılan parola *safetica* 'dır.
6. Bir lisans anahtarınız varsa bunu, *Management and settings -> License Manager* sekmesinden girin. Lisans yalnızca (SEC)'e uygulanır. Safetica fonksiyonları istemciye uygun modül için lisans atadığınızda aktif olacaktır. Bu işlem, istemci kurulup sunucuya bağlandıktan sonra aynı yerden yapılabilir.

SMS'in detaylı anlatımı:

1. Konsola ilk kez bağlanıldığında, bir oturum açma penceresi belirir ve bir yerel parola girmenizi ister. Parola, konsol erişiminizi korur. SMS'e bağlantıyla bir ilgisi yoktur.

Yeni bir parola girdikten sonra "parolayı hatırla" seçeneğini işaretleyip onaylayın.

SMC'ya bağlanmak istediğinizde bu parolayı girmeniz gerekecek. SMC parolası *Management and settings* -> *Console settings* altından değiştirilebilir.

- Şimdi yeni SMS'e bağlanmanız gerekir. *Management and settings* -> *Server settings*'i açın. "New server"a tıklayın ve SMS'in çalıştığı bilgisayarın adresini domain formunda (server.com) ya da IP adresi olarak girin (eğer birden fazla SMS varsa birini seçin). SMS'in çalıştığı portu da belirleyebilirsiniz. Varsayılan olarak bu port 4441'dir. Bu portu STAService.exe -adminport <yeni port numarası> komutunu Administrator olarak SMS'in kurulduğu konumda komut satırından girerek değiştirebilirsiniz. Port değişikliği SMS yeniden başlatıldıktan sonra gerçekleşecektir.

Her SMS önceden tanımlı bir administrator hesabıyla gelir. Aşağıdaki kullanıcı bilgileri ile oturum açabilirsiniz:

Username: *safetica*

Password: *safetica*

Bunları ilgili alanlara girin. SMS'e bağlanıp SMC'yi çalıştırdıktan sonra bu hesabın şifresini, *Management and settings* -> *Server Settings* ya da *Management and settings* -> *Access management* kısımlarından değiştirebilirsiniz.

The screenshot shows the Safetica Management Console interface. The top navigation bar includes 'Safetica Management Console' and various icons for Auditor, DLP, Supervisor, Dashboard, Alerts, Reports, and Management and settings. The main content area is titled 'Server settings' and contains several sections:

- BASIC INFORMATION**: A section with a 'Hide' button and a help icon. It contains text explaining that server settings allow setting connections to one or more SMS, including database connections, AD synchronization, and SMTP server for e-mails.
- CONNECTION TO SAFETICA MANAGEMENT SERVICE**: A section with 'New server', 'Edit', and 'Remove' buttons. It contains a table with one entry: Service: 192.168.29.135, Username: safetica.
- Version and name**: A section with a 'Hide' button. It shows 'Version: 5.0.0' and 'Server Name: SMS'. A note states: 'The name of the server provides a unique server identification throughout Safetica'.
- Databases connection settings**: A section with a 'Hide' button. It includes fields for 'Database' (Main database), 'Server' (192.168.29.135), 'Port' (1433), 'Database name' (ses5_main_RC), 'Username' (sa), and 'Password' (masked). A 'Test connection' button is also present. A note says: 'Enter a server address reachable from all client computers.' A link for 'Safetica Data Calculator' is provided: <http://calc.safetica.com/>.
- ACTIVE DIRECTORY**: A section with a 'Hide' button. It has an 'Add' button and a 'Connected nodes' field.

- Giriş bilgisini onayladıktan sonra, SMC SMS'e bağlanır. Bir bağlantı kurulduğunda, SMS sertifika uyarısı penceresi belirir. "Yes"i tıklayarak devam edin.


Bu tür kurulum SQLite kullanır ve database'ler SMS kurulumu sırasında otomatik olarak

oluşturulur. Açılır liste menüsü herbir database'deki dosyalara erişim yollarını görüntülemenizi sağlar.

Main database – Safetica.db – konsol, kullanıcılar ve bilgisayarlar için ayarları içerir.

Log database – Log.db – izleme ile toplanan kayıtları ve logları içerir.

Category database – Categories.db – Ugulamaların, web sayfalarının ve dosya uzantılarının kategorilerini, loglarını ve kayıtlarını içerir.

Burada herşey zaten ayarlanmış olmalıdır. Yapılan tüm ayarlamalar butonuna basarak kaydedilir. 

Database'lerdeki veri boyutu

İzleme sonucu biriken data boyutu esas olarak, sistemi üzerine kurduğunuz kullanıcı sayısına ve Safetica'nın etkinleştirdiğiniz modüllerinin miktarına bağlıdır. Bu kriterlere göre yaklaşık bir tahmine <http://calc.safetica.com/> adresinde bulabileceğiniz bir hesaplama aracı ile ulaşabilirsiniz.

4. Firma ağınıza birden fazla SMS kurduysanız, yukarıda bahsedilen aşamaları her biri için tekrarlamanızı öneririz. Başka bir SMS'e bağlanmak için sunucu ayarlarını tekrar görüntüleyin; bu ana SMC menüsünde *Management and settings* -> *Console settings*'e girerek görüntülenebilir. "New server" butonuna tıklayın ve bağlantı bilgisini girin. Her bir SMS'e bağlantı için konsolu kullanın. Öncelikle varsayılan yönetici hesabının parolasını değiştirin ve ardından *Management and settings* -> *Access management* içerisinden firma ilkelerinize göre uygun yetkilere sahip SMS erişim hesapları oluşturun. Her SMS kendi ayrı erişim hesaplarına sahiptir.

Muhtemel erişim hesapları ve bunların yetkileri için örnekler:

Güvenlik Yöneticisi – DLP ve Supervisor modül ayarlarına erişebilir. Çalışanların izlenmesiyle edinilen hiç bir datayı göremez.

Müdür – tüm modülerden gelen görüntüleme verisine erişebilir ancak hiç bir ayarı değiştiremez.

Denetleyici – Auditor modülünün ayarlarını değiştirebilir ve çalışanların izlenmesi ile edinilen verileri görüntüleyebilir.

Tabi ki her SMS için oluşturduğunuz kullanıcıların haklarını dilediğiniz gibi düzenleyebilirsiniz. Hesap ayarları ve her modül için erişim hakları düznlme için Access management kısmına bakınız.

5. Şimdi güncel bir kategori database'i indirmeniz gerekmektedir. SMC'nin ana menüsünden "Management and settings -> Categories -> Update"e gidin. Aşağıdaki üç seçeneği içeren bir pencere açılacak:
 1. İnternette güncelleme (service'e) – database güncelleme SMS sunucu service'i tarafından yapılır. Güncelleme esnasında ilerlemeyi gösteren bir pencere açılır.

Not: Bu seçenek için Safetica Management Service'in internet erişimi olmalıdır.
 2. Klasörden güncelleme (service'e) – database güncelleme harddisk üzerinde bir güncelleme klasöründen yapılır. Bu metod internet erişiminiz olmadığında ve indirilmiş güncelleme dosyası bulunduğu uygundur. Girmeniz gereken yol, SMS çalıştıran bilgisayar üzerindeki güncelleme dosyasının yoludur. SMC Konsolunu çalıştırdığınız bilgisayar üzerinde bir yol değildir.
 3. Güncellemeleri indirme (konsola) – Güncelleme dosyası web sunucusundan bilgisayarınıza indirilir. Dosyayı sunucu servisine elle ya da yukarıda bahsedilen

"klasörden güncelleme" yoluyla yüklenebilir. İlerlemeyi gösteren bir pencere açılacaktır.

Kurulumun bu kısmı mecburi değildir ancak bu işlem gerçekleştirilene kadar bir çok fonksiyon aktif olmayacaktır.

6. Safetica Endpoint Client'ın (SEC) yerel yönetim şifresini değiştirin – bkz. Safetica Endpoint Client'a yetkisiz müdahale. Önce de olduğu gibi varsayılan parolanız *safetica 'dır*.
7. Son olarak da kullanıcılara modül lisanslarını atamanız gerekmektedir. Bunu Management and settings -> License Manager altından SMC.

License Manager'a anahtarınızı girin ve onayladıktan sonra, orta kısımda kullanıma müsait lisansların sayısını göreceksiniz. Daha sonra lisansları gruplara, kullara ya da kullanıcılara atayabilirsiniz. Bu şekilde hangi grup ya da kol tarafından ne kadar lisans kullanılabileceğini kontrol altına almış olursunuz. Yeni bir SEC'i SMS'e (database) bağladığınızda, atanmış olan lisans istemciye indirilecek ve License Manager'daki boş lisans adedi buna bağlı olarak azalacaktır. Lisans yönetimi hakkında daha fazla bilgiyi License Manager kısmından edinebilirsiniz.

Ayrıca, Safetica Endpoint Client'ın kaldırılması, güncellenmesi ya da kapatılması için parolalarınızı değiştirmenizi şiddetle tavsiye ediyoruz. Bunu, Management and settings -> Client settings sekmesindeki Allowed actions kısmından yapabilirsiniz. Daha fazla bilgi için Safetica Endpoint Client Protection' a bakınız.

3.2.5 Safetica Endpoint Client kurulumu

Safetica Endpoint Client (SEC) Safetica'nın kurulacak son bileşenidir. Client makinalarda güvenlik ilkelerinin uygulanmasını ve Safetica Management Console (SMC) üzerinde yapılandırılmış olan ayarların bu makinalar üzerinde düzgün çalışmasını sağlayan esas bir bileşendir. Son kullanıcılar için, ayrıca bir dizi güvenlik aracı sağlar.

Kurulumu aşağıdaki gibi devam edin:

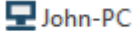

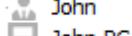

1. İndirmiş olduğunuz kurulum paketini açın. Dilinizi seçerek lisans koşullarını kabul ettikten sonra *Installation -> Small Installation -> Safetica Endpoint Client* yolunu izleyin.
2. Burada iki seçeneğiniz var.
 - o Setup'ı direkt olarak kurulum paketinden çalıştırın, "Run installer" butonu.
 - o Yalnızca SEC installer'ı çıkartın, bunu daha sonra kurulum için kullanabilirsiniz.
3. Kurulumu çalıştırdıktan sonra (kurulum paketinden ya da dışarı çıkarttığınız yerden), dilinizi bir kez daha seçerek lisans koşullarını kabul edin.
4. Kurulum klasörünü seçin.
5. "*Enable network mode*" kutucuğunun işaretli olduğundan emin olun ve SMS'i çalıştıran bilgisayarın adresini girin. Client'ın bağlanacağı server'ı belirlemiş oluyorsunuz. Safetica Management Service üzerinde değiştirdiyse port numarasını değiştirin; aksi takdirde varsayılan port olan 4438'i bırakın.
6. Kurulumu tamamladıktan sonra, STCService.exe servisinin çalıştığından (Windows Görev Yöneticisi > Servisler > STCService – çalışıyor) emin olun.
7. Son olarak güvenlik duvarınızda ve anti-virüs yazılımınızda şunlar için izinler tanımlayın: STCService.exe, STPCLock.exe, STMonitor.exe, STUserApp.exe, ve Safetica.exe.

SEC'i yapılandırmak için, Safetica ürününün geneli için olduğu gibi, [After Installation](#) kısmını okuyarak devam edin.

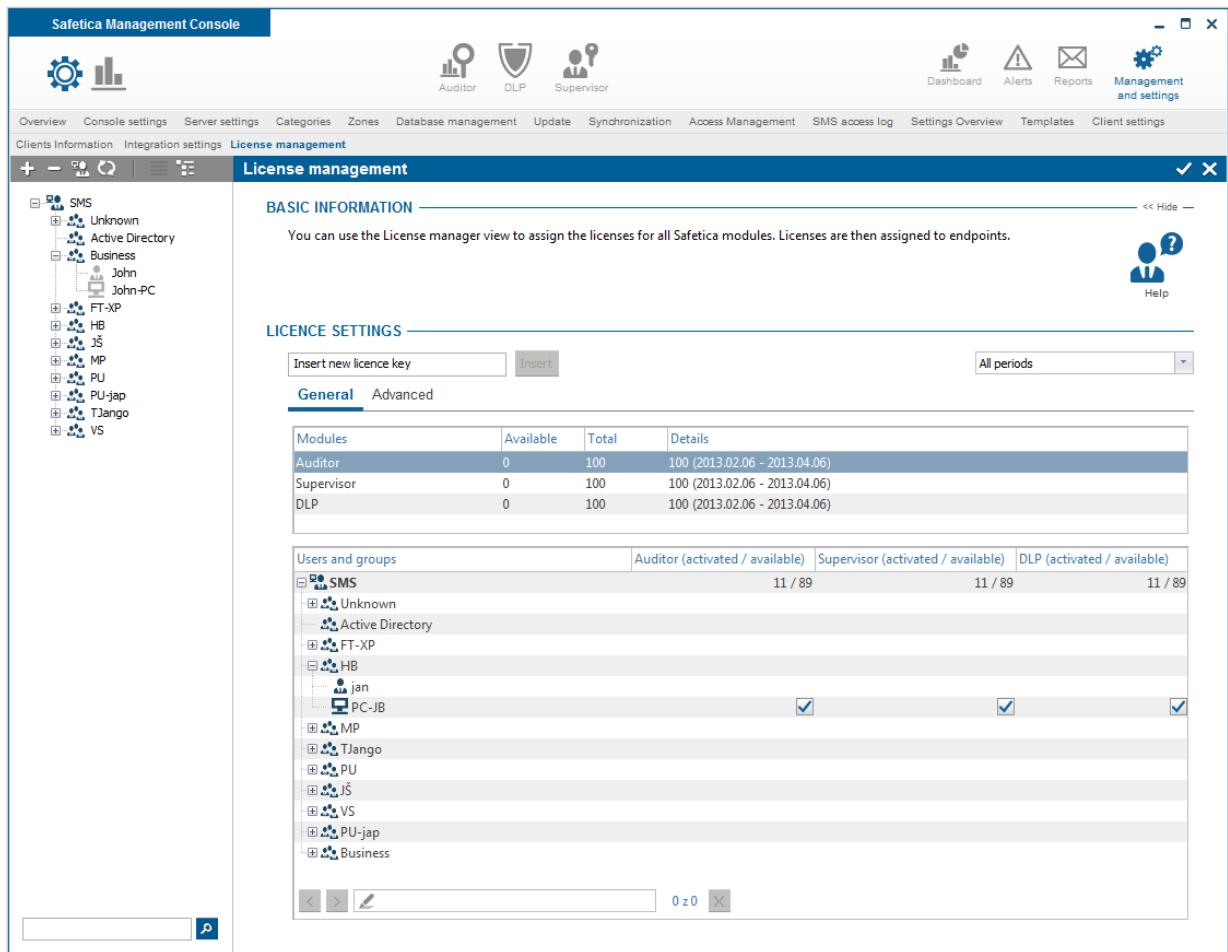
3.2.6 Kurulumdan Sonra

Tüm Safetica bileşenlerini kurduktan sonra, Safetica'yı kullanmaya başlamadan önce yapmanız gereken son birkaç dokunuş kaldı.

1. Öncelikle tüm Safetica Endpoint Client'larının (SEC) sunucuya bağlandığından emin olun - Safetica Management Server (SMS)-. Kullanıcı ağacında, kullanıcılar ve bilgisayarlar renklerle ifade edilir.

-  John-PC
○  John SEC online ve SMS'e bağlı.
-  John-PC
○  John SEC offline ve SMS'e bağlı değil.

2. İstemcilere ilgili modülleri atamak için License Manager'ı kullanın. Kendisine lisans atanan her bilgisayar ve modül bir "tik" ile gösterilecektir. Atanmış lisanslar olmaksızın, modül özellikleri aktif olmayacaktır.



License management

BASIC INFORMATION

You can use the License manager view to assign the licenses for all Safetica modules. Licenses are then assigned to endpoints.

LICENCE SETTINGS

Insert new licence key All periods

General **Advanced**

Modules	Available	Total	Details
Auditor	0	100	100 (2013.02.06 - 2013.04.06)
Supervisor	0	100	100 (2013.02.06 - 2013.04.06)
DLP	0	100	100 (2013.02.06 - 2013.04.06)

Users and groups

	Auditor (activated / available)	Supervisor (activated / available)	DLP (activated / available)
SMS	11 / 89	11 / 89	11 / 89
Unknown			
Active Directory			
FT-XP			
HB			
jan			
PC-JB	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MP			
TJango			
PU			
JS			
VS			
PU-jap			
Business			

3. DLP modülüne bir lisans atadıysanız, Client GUI mode'unu seçin. Varsayılan olarak, çalışanlarınız Endpoint Security Tools özelliklerine erişebilir (Normal mode). Üç mod arasından seçim yapabilirsiniz (DLP -> Endpoint Security Tools settings -> Client GUI mode):
 - Normal – güvenlik araçları ve içerik menüsü içeren bir Endpoint Security Tools kullanıcı arayüzü.
 - Tray only – kullanıcılar yalnızca içerik menüsünden erişilebilen temel fonksiyonlara ulaşabilir. Kullanıcı arayüzü yok.
 - Invisible – kullanıcılar ne içerik menüsüne ne de Endpoint Security Tools fonksiyonlarına erişebilir.

BASIC INFORMATION << Hide

Endpoint Security Tools (EST) are part of Safetica Endpoint Client and are available only when there is a valid Safetica DLP licence. The user can utilize EST to manage the encrypted disks, use the data shredder or the password database. In the following sections you can set basic security settings for EST at endpoint to force the appropriate security level.

**SYSTEM SETTINGS**

Run on system startup: Inherit

Associate .dco, .dcf and .dcd files with Safetica: Inherit

DISK AND ENVIRONMENT SETTINGS

Client GUI mode: Inherit

Forced disk unmounting: Inherit

Access to connected disks: Inherit

Forced disk unmounting hotkey (Win-Ctrl-Q): Inherit

Disk unmounting hotkey (Win-Ctrl-U): Inherit

SECURITY RULES

Data shredder mode: Inherit

Forced disk password change: Inherit

Change password every: days

Passwords remembering: Inherit

Minimum password level: Inherit

Enforce these settings on client: Inherit

Düzgün veri aldığınızdan emin olabilmek için bazı fonksiyonları etkinleştirmeyi deneyin (örn. Application monitoring)

Bu noktada Safetica kullanıma hazırdır.

