WEBROOT®

SecureAnywhere Zakelijk
Global Site Manager
Beknopte handleiding

Inhoudsopgave

Webroot SecureAnywhere – Zakelijk

De implementatie van Webroot SecureAnywhere voor bescherming van zakelijke endpoints (WSAB) is eenvoudig met onze GSM-console (Global Site Manager), maar we weten dat omgevingen sterk kunnen verschillen en dat elke implementatie andere vereisten heeft. Vanuit die wetenschap worden in deze Beknopte handleiding enkele veelvoorkomende implementatiescenario's en -instellingen beschreven. De informatie moet zoals altijd worden afgewogen tegen uw specifieke implementatieomgevingen en beveiligingsbeleid.

Vereisten

Toegangsvereisten voor beheerconsole

- Internettoegang is vereist.
- Google Chrome® (32-bits en 64-bits); huidige versie en vorige twee versies
- Internet Explorer® (32-bits en 64-bits); versie 11
- Microsoft Edge® (32-bits en 64-bits; huidige versie en twee vorige versies
- Mozilla® Firefox® (32-bits en 64-bits; huidige versie en twee vorige versies
- Safari; huidige versie en twee vorige versies
- Opera; huidige versie en twee vorige versies

WSAB-agent: systeemvereisten

Werkstations

- Windows 10 (32-bits en 64-bits)
- Windows 8 en 8.1 (32-bits en 64-bits)
- Windows 7 (32-bits en 64-bits), Windows 7 SP1 (32-bits en 64-bits)
- Windows Vista® (32-bits), Windows Vista SP1, SP2 (32-bits en 64-bits)
- Mac OS X 10.7 (Lion®)
- Mac OS X 10.8 (Mountain Lion®)
- OS X 10.9 (Mavericks®)
- OS X 10.10 (Yosemite®)
- OS X 10.11 (El Capitan®)
- macOS 10.12 (Sierra®)
- macOS 10.13 (High Sierra®)

Server

- Windows Server 2003 Standard, Enterprise, 32-bits en 64-bits
- Windows Server 2008 R2 Foundation, Standard, Enterprise
- Windows Small Business Server 2008 en 2011
- Windows Small Business Server 2012

Virtuele serverplatforms

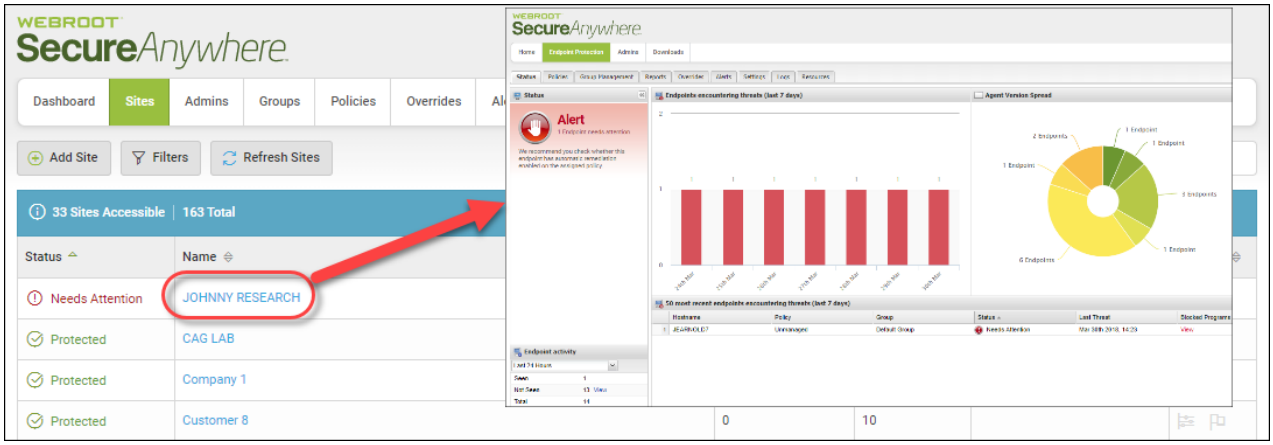
- VMware vSphere 4 (ESX/ESXi 3.0, 3.5, 4.0, 4.1), Workstation 6.5, 7.0 en Server 1.0, 2.0
- Citrix XenDesktop 5 en XenServer 5.0, 5.5, 5.6
- Microsoft Hyper-V Server 2008, 2008 R2

Serviceconfiguraties

Global Site Manager (GSM) van Webroot is een in de cloud gehoste, hiërarchische beheertool die een intuïtieve interface biedt voor het beheer van meerdere entiteiten, zoals geografische locaties, sites en gebruikersgroepen.

Elke entiteit binnen Global Site Manager kan uniek worden geïdentificeerd aan de hand van de eigen sleutelcode en kan indien nodig ook afzonderlijk worden beheerd met behulp van een eigen WSAB-beheerconsole voor endpointbescherming.

Met Global Site Manager kunnen ook algemeen beleid, tijdelijke uitschakelingen en waarschuwingen voor alle endpointentiteiten worden afgedwongen.



De standaard WSAB-beheerconsole voor endpointbescherming is een in de cloud gehoste oplossing die extern endpointbeheer biedt, inclusief beleids- en groepstoewijzing, rapportage, controlelogbestanden en waarschuwingen.

Er wordt in dit document van een aantal zaken uitgegaan:

- U hebt de welkomste-mail ontvangen. Zie voor meer informatie de Beknopte handleiding Endpoint-bescherming voor kleine en middelgrote bedrijven.

  Opmerking: als u de welkomste-mail niet hebt ontvangen, neemt u contact op met uw Webroot-partner of informeert u uw Webroot-kanaalaccountmanager.

- U hebt uw gebruikerslogin voor de beheerconsole ingesteld.
- U hebt rechtstreeks toegang tot Webroot SecureAnywhere Global Site Manager.

Algemene instelling

Er zijn meerdere manieren om de WSAB-service in te stellen, afhankelijk van uw behoeften en vereisten:

Scenario 1: Alle beheerde entiteiten binnen één WSAB-console voor endpointbescherming.

- Dit is ideaal voor meerdere entiteiten die *geen* afzonderlijke beheertoegang via een eigen persoonlijke console nodig hebben.
- Elke entiteit wordt vervolgens eenvoudig ingesteld onder een afzonderlijke groepsnaam. De groepsnaam wordt tijdens de installatie opgegeven.

Scenario 2: Alle entiteiten binnen de WSAB Global Site Manager-console.

- Deze aanpak is geschikt voor grote implementaties voor veel verschillende entiteiten en een groot aantal endpoints die beheer op maat vereisen.
- Als afzonderlijke entiteiten een niveau van lokale beheertoegang tot hun lokale console nodig hebben.
- Voor situaties waarin u beheerderstoegang tot bepaalde lokale functies moet beperken.

Scenario 3: Hybride aanpak.

- Enkele gegroepeerde entiteiten binnen één WSAB-console voor endpointbescherming
- Enkele klanten in Global Site Manager, op verschillende locaties

Opmerking: de manier waarop u WSAB beheert, is uiterst flexibel. U kunt het beheer afstemmen op uw implementatie, entiteitidentificatie (sleutelcode) en beheerbehoeften.

Implementatie

Gebruik de volgende tabel om de juiste stappen voor uw implementatieproces te bepalen.

Als u dit doet…	Doet u dit…
Alle entiteiten binnen één WSAB-console voor endpointbescherming selecteren.	Raadpleeg de Beknopte handleiding WSAB-EP.
Alle entiteiten in Global Site Manager selecteren.	Lees verder.
Een hybride aanpak selecteren.	Lees verder.

Algemeen implementatieproces

- GSM-site maken
  - Eén site voor elke entiteit
  - Eén site voor meerdere entiteiten, indien van toepassing
- Beleid maken/toewijzen
- Aanvullende beheerders maken en machtigingen toewijzen, indien van toepassing
- WSAB-URL's toestaan, indien van toepassing
- Algemene waarschuwingen configureren, indien van toepassing
- WSAB-agent implementeren

Opmerking: zie voor meer informatie de GSM Beheerdershandleiding.

Beleid

Beleid biedt een beheerder gecentraliseerde controle over de WSAB-instellingen van een endpoint. Beleid kan worden geconfigureerd op het niveau van de GSM en/of de entiteit. Zie voor meer informatie het gedeelte Werken met beleid van de GSM Beheerdershandleiding.

Beleid kan op verschillende locaties binnen SecureAnywhere worden geconfigureerd:

- GSM-beleid of algemeen beleid kan worden geconfigureerd op het GSM-niveau en kan op een of meer entiteiten worden toegepast.
  - Beleid wordt geconfigureerd op het tabblad Beleid.
  - Er kan een standaardbeleid aan een GSM-site-entiteit worden toegewezen wanneer de site wordt gemaakt of door instellingen van een site te bewerken.
- Sitebeleid kan worden geconfigureerd op het niveau van de site.
  - Beleid wordt geconfigureerd op het tabblad Beleid.
  - Er kan standaardbeleid worden ingesteld.
  - Beleid kan op het tabblad Groepenbeheer aan groepen worden toegewezen.
  - Endpoints in deze groepen nemen het toegewezen groepsbeleid over.

Webroot SecureAnywhere bevat vier aanpasbare beleidsregels:

- **Aanbevolen standaardinstellingen**: aanbevolen instellingen met endpointbescherming en herstel ingeschakeld.
- **Aanbevolen standaard serverinstellingen**: aanbevolen instellingen voor gebruik op servers, met bescherming en herstel ingeschakeld.
- **Stille controle**: geen herstel, alleen rapportage over beveiligingscontrole.
- **Onbeheerd**: biedt agentbeleidscontrole aan de endpointgebruiker.

Opmerking: wanneer een endpoint onder een ander beleid dan Onbeheerd valt, wordt het automatisch vergrendeld, wordt de agent beschermd tegen fraude en worden wijzigingen of verwijdering voorkomen. Standaardbeleid kan niet worden bewerkt of verwijderd. Het kan wel worden gekopieerd en bewerkt om nieuw aangepast beleid te maken.

Het aanroepinterval

De WSAB-EP-agent logt bij de console in wanneer de volgende evenementen zich voordoen:

- Het configureerbare, door beleid toegewezen aanroepinterval verloopt.
- Zowel gescande als handmatige scans worden uitgevoerd.
- Er wordt een nieuw bestand bepaald.
- Het endpoint wordt opnieuw opgestart.
- Met de rechtermuisknop op de WSAB-agent klikken in het systeemvak en Configuratie vernieuwen kiezen.
- Een agentaanroep wordt geactiveerd met behulp van de externe agentopdrachtregel. Raadpleeg voor meer informatie over externe opdrachten Schakelopties op de opdrachtregel.

Installatieopties

- Windows
  - EXE-pakket
  - MSI-pakket
- Mac
  - DMG-pakket

Opmerking: alleen afzonderlijke 'onderliggende' sleutelcodes voor de entiteit/site moeten worden gebruikt voor implementatie. De sleutelcode van de 'bovenliggende' GSM-account moet nooit worden gebruikt.

- Er is een aangepast EXE-pakket beschikbaar op het niveau van de onderliggende sleutelcode van de site, onder de link Bronnen > Windows-download. De naam van het EXE-pakket van de site wordt dan gewijzigd met behulp van de verschafte sleutelcode. Wanneer het wordt uitgevoerd wordt de sleutelcode ingesloten in het onbeheerde installatieproces op de achtergrond.
- De MSI kan rechtstreeks worden bewerkt, zodat deze de sleutelcode van de site bevat, en worden geïmplementeerd met behulp van Windows-groepsbeleid, RMM of een softwaredistributiemethode die een MSI-pakket ondersteunt.

Installatie op VM's/Citrix

Sommige architecturen kunnen duplicaten in de WSAB-console veroorzaken. Dit kan soms voorkomen vanwege onjuist geconfigureerde endpointimages of virtuele machines.

Als tijdens testen duplicaten optreden in uw Webroot-console, verwijdert u Webroot SecureAnywhere voor bescherming van zakelijke endpoints uit de betrokken endpoints. Installeer het vervolgens opnieuw met de opdrachtregeloptie *-clone*, waardoor SecureAnywhere een unieke identificatie voor dat systeem maakt.

Voer bijvoorbeeld de volgende opdrachtregel in:

WSABsme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -clone

Opmerking: de X'en staan voor de cijfers in uw licentiesleutel.

Na de installatie wordt een nieuwe hostnaam weergegeven in de Webroot-console. Hostnaam *PCHOSTNAME* wordt bijvoorbeeld *PCHOSTNAME-C8137921*.

Wanneer een agent wordt verwijderd of opnieuw wordt geïnstalleerd, blijft deze waarde bestaan, zodat bestaande agents niet naar andere ID's worden verplaatst. Als het besturingssysteem opnieuw wordt geïnstalleerd, verandert de ID echter wel.

Tijdelijke uitschakelingen

Tijdelijke uitschakelingen geven een beheerder gecentraliseerde controle over de bestanden die mogen worden uitgevoerd op endpoints, en de mogelijkheid bestanden te overschrijven als *Goed* of *Slecht*. Tijdelijke uitschakelingen kunnen worden geconfigureerd op het niveau van de GSM-console en/of de siteconsole.

Raadpleeg voor meer informatie het hoofdstuk Working With Overrides in de Global Site Manager Admin Guide.

Tijdelijke uitschakelingen kunnen op verschillende locaties binnen SecureAnywhere worden geconfigureerd:

- GSM-beleid of algemene uitschakelingen kunnen worden geconfigureerd op het GSM-niveau en kunnen op een of meer sites worden toegepast.
    - Onder Algemene instellingen > Tijdelijke uitschakelingen.
    - Tijdelijke uitschakelingen kunnen worden geconfigureerd met de MD5 van een bestand.
    - Tijdelijke uitschakelingen kunnen worden geïmporteerd uit de bestaande tijdelijke uitschakelingen van een site.
- Tijdelijke uitschakelingen van een site kunnen worden geconfigureerd op het siteniveau en kunnen worden toegepast op een hele site of op één beleid:
    - Op het tabblad Tijdelijke uitschakelingen.
    - Tijdelijke uitschakelingen kunnen ook op de tabbladen Status, Groepenbeheer en Rapporten worden geconfigureerd met de knop Tijdelijke uitschakeling aanmaken:

Ondersteuning

Logboeken verzamelen

Het openen van een ondersteuningsticket kan meestal worden versneld door eerst logbestanden te verzamelen vanuit het betrokken endpoint.

Agentopdracht Klantendienstdiagnoses

Gebruik van de WSAB-agentopdracht `Klantendienstdiagnoses` is de methode die de voorkeur heeft.

Met deze agentopdracht wordt alle benodigde diagnostische informatie verzameld die het ondersteuningsteam van Webroot nodig heeft om u te helpen met het probleem.

Als u dit proces nog meer wilt versnellen, klikt u op het endpoint op de knop **Configuratie vernieuwen**, in plaats van te wachten tot het aanroepinterval voor het endpoint verstrijkt om in te loggen en de agentopdracht op te halen.

Locatie van logbestanden

WSAB-EP-logbestanden bevinden zich in de map WRData:

- Windows XP-systemen: C:\Documents and Settings\All Users\WRData
- Windows Vista en nieuwer: C:\ProgramData\WRData

Ondersteuningstickets openen

Ondersteuning kan worden verkregen via het web of de telefoon:

http://www.webroot.com/us/en/support/support-business

Communicatie

De WSAB-agent communiceert via poort 80 en 443 met het Webroot Intelligence Network en uw beheerconsole. Deze communicatie wordt verborgen door een merkgebonden vorm van versleuteling. Als u een webinhoudsfilter of een proxyserver gebruikt, kunt u het volgende overwegen om te zorgen dat de WSAB-agent kan communiceren met het Webroot Intelligence Network en uw console.

Voor WSAB benodigde URL's

Wanneer u firewalls configureert of een netwerklaag die WSAB-verkeer kan blokkeren, overweeg dan de volgende URL-maskers. Deze URL's kunnen ook worden gebruikt om systemen te vergrendelen die anders helemaal geen internet zouden hebben.

Pad	Poort	Informatie
***.webrootcloudav.com**	Poort 443 (https)	Agentcommunicatie en -updates. **Opmerking:** sommige firewalls ondersteunen geen subdomeinnamen met twee punten die worden voorgesteld door één jokerteken, bijvoorbeeld als g1.p4.webrootcloudav.com wordt voorgesteld door *.webrootcloudav.com. Deze omgevingen vereisen dus *.p4.webrootcloudav.com of *.*.webrootcloudav.com.
***.webroot.com**	Poort 443 (https)	Agentberichten.
***.webrootanywhere.com**	Poort 443 (https)	Downloaden en uploaden van bestanden door agent.
https://wrskynet.s3.amazonaws.com/*	Poort 443 (https)	Downloaden en uploaden van bestanden door agent.
https://wrskynet-eu.s3-eu-west-1.amazonaws.com/*	Poort 443 (https)	Downloaden en uploaden van bestanden door agent.
https://wrskynet-oregon.s3-us-west-2.amazonaws.com/*	Poort 80 (http) en 443 (https)	Vereist voor agentwebfiltering; elasticbeanstalk is een Amazon AWS-domein.
WSAWebFilteringPortal.elasticbeanstalk.com	Poort 80 (http) en 443 (https)	Beheerportal en uploaden van logboeken voor ondersteuningstickets.

URL voor Mobiele bescherming

Als u Mobiele bescherming hebt, moet u de volgende URL toestaan:

- *.webrootmobile.com

Systeeme-mailadressen

Als u zeker wilt weten dat u e-mails van de onderstaande adressen ontvangt, wordt het aanbevolen deze toe te voegen aan uw toegestane/witte lijsten:

- Welkomste-mail: noreply@webroot.com
- Waarschuwingen/overzichten: noreply@webrootanywhere.com
- Ondersteuningsberichten: noreply@webrootcloudav.com

Proxyinstellingen

1. Als u de schakeloptie `–autoproxy` gebruikt tijdens de installatie, detecteert de WSAB-agent automatisch de proxyinstellingen van een endpoint.
2. U kunt deze instellingen indien nodig echter ook handmatig opgeven. De syntaxis wordt beschreven onder Schakelopties op de opdrachtregel.

Schakelopties op de opdrachtregel

Opdrachtregel	Omschrijving
/key	Installeren met een specifieke sleutelcode. Voorbeeld: `WSABsme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx`
/silent	Op de achtergrond installeren, zonder aanwijzingen weer te geven. Voorbeeld: `WSABsme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent`

Opdrachtregel	Omschrijving

/group=GROEPSCODE	Schakeloptie op de opdrachtregel voor rechtstreekse implementatie naar groepen.
	Voorbeeld:
	`WSABsme.exe /key=xxxxxxxxx /group=-135260017840748808 /silent`
	Endpoints aan een specifieke groep toewijzen door de groep te selecteren waaraan u endpoints wilt toevoegen, en vervolgens in het vervolgkeuzemenu Acties de optie Endpoints implementeren in deze groep te selecteren. Let op de GROEPSCODE.
	Overige vereisten:
	• De groep moet al bestaan in de console.
	• Dit werkt alleen voor nieuwe installaties op systemen die nog nooit eerder door de console zijn gezien.
	Voorbeeld van opdrachtregel:
	`msiexec /i "C:\WSABsme.msi" GUILIC="XXXX-XXXX-XXXX-XXXX" CMDLINE="SME,quiet,Group=-135260017840748808" /qn /l*v %windir%\WSAB_install_log.txt`
	Voor MSI-installaties kunt u de opdrachtregel en een MSI-editor gebruiken.
	Voorbeeld van MSI-editor in veld CMDLINE: Group=-135260017840748808

-clone	Gebruiken wanneer InstanceMID's overeenkomen, waardoor duplicaten ontstaan in de console of endpoints andere endpoints vervangen bij elk aanroepinterval; meestal aangetroffen in imageomgevingen of gekloonde omgevingen. Voorbeeld: `WSABsme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -clone`
-uniquedevice	Gebruiken wanneer DeviceMID's overeenkomen, waardoor duplicaten ontstaan in de console of endpoints andere endpoints vervangen bij elk aanroepinterval. Meestal gebruikt voor virtuele omgevingen zoals Citrix Provisioning of VDI, waarin het gebruik van -clone niet effectief is omdat de DeviceMID's hetzelfde zijn. Voorbeeld: WSABsme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -uniquedevice

Opdrachtregel	Omschrijving
-poll	Aanroepen met behulp van een opdrachtregeloptie. Voorbeeld: `"c:\program files\webroot\wrsa.exe" -poll`
-autoproxy	De automatische proxyconfiguratie gebruiken.

-proxy	Proxyinstellingen.
	Gebruik altijd alle parameters en maak elke waarde die u niet nodig hebt, leeg met dubbele aanhalingstekens, bijvoorbeeld proxypass=""
	proxyauth # being:
	0 = Elke verificatie
	1 = Basis
	2 = Digest
	3 = Onderhandelen
	4 = NTLM
	Voorbeeld:
	`WSABsme.exe /key=xxxx-xxxx-xxxx-xxxx-xxxx /silent -proxyhost=nn.nn.nn.nn -proxyauth=n -proxyuser="proxygebruiker" -proxypass="wachtwoord" -proxyport=port_number`

Tips voor verwijdering

Optie #1: verwijderen met behulp van agentopdrachten

1. Open het tabblad Groepenbeheer en selecteer een groep in het paneel Groepen.
2. Voer een van de volgende handelingen uit:
   - Selecteer een afzonderlijk endpoint waarop u de opdracht wilt uitvoeren.
   - Als u de opdracht op alle endpoints wilt uitvoeren, selecteert u **Hostnaam**.
3. Open het menu Agentopdrachten en selecteer **Agent > Verwijderen**.

   De WSAB-agent wordt verwijderd; de vermelding voor het werkstation blijft echter staan. Het wordt aanbevolen een groep met de naam Verwijderde clients te maken waarnaar u deze clients kunt verplaatsen.

   Als u een vermelding helemaal wilt verwijderen, selecteert u de rode knop **Deactiveren**. Hiermee wordt het licentiewerkstation vrijgegeven dat door het endpoint in beslag wordt genomen.
   Dit endpoint wordt niet meer ingelogd bij uw console, tenzij u het weer activeert.

Optie #2: verwijderen in veilige modus met netwerken

Gebruik de volgende stappen om de computer op te starten in de veilige modus met netwerken.

1. Zet de computer uit.
2. Zet de computer aan en druk de toets **F8** herhaaldelijk in.
3. Gebruik de pijlen **Omhoog** en **Omlaag** om **Veilige modus met netwerken** te selecteren.
4. Druk op **Enter** op het toetsenbord.
5. Voer een van de volgende handelingen uit:
   - Als het endpoint met een beleid werd beheerd, selecteert u **Veilige modus met netwerken**. Dit is de standaard.
   - Als het endpoint niet met een beleid werd beheerd, selecteert u **Veilige modus**.
6. Voer een van de volgende handelingen uit, afhankelijk van uw besturingssysteem:
   - **Windows XP**: klik op **Start** en vervolgens op **Uitvoeren**. Typ in het venster Uitvoeren **appwiz.cpl** en druk vervolgens op **Enter** op het toetsenbord.
   - **Windows Vista en nieuwer**: klik op **Start** of op het **Windows**-pictogram. Typ in het veld Zoeken **appwiz.cpl** en druk vervolgens op **Enter** op het toetsenbord.
7. Selecteer **Webroot SecureAnywhere** en klik vervolgens op **Verwijderen**.
8. Bevestig eventuele berichten over verwijdering van het programma.

   Wanneer de verwijdering is voltooid, start u de computer opnieuw op.

   Als Webroot SecureAnywhere niet zichtbaar is in het Configuratiescherm, kunt u de software vanaf de opdrachtregel verwijderen door het volgende uit te voeren: *C:|Program Files|Webroot|WRSA.exe –uninstall*

Bronnen

Links

- WSAB-console
- Vraag het aan Webroot
- Ondersteuningsticket openen
- Zakelijke gemeenschap
- Beheerdershandleiding
- Webroot YouTube Channel
- WSAB-probeerversie

Demo's

- http://detail.webrootanywhere.com/gsmdemo_sites.asp
- http://detail.webrootcloudav.com/Endpoint_demo.asp