End Point Control (EPC) for the SRA Series for SMB

Endpoint interrogation and control for the SRA Series

IT departments of small- to medium-sized businesses (SMBs) are increasingly embracing Bring Your Own Device (BYOD) initiatives, and allowing employees and partners to connect their own devices to the corporate network. However, introducing non-IT-managed devices into the network raises real concerns that these endpoints could potentially become conduits for harmful malware.

To address these concerns, SMB IT departments need a solution that uniquely identifies and verifies the device integrity of remote endpoints before authorizing their access to the network. This is especially important for the Windows®-based laptops and netbooks commonly found in SMBs. Unfortunately, few SSL VPN vendors even offer endpoint control for these smaller organizations.

Dell™ SonicWALL™ End Point Control (EPC) for the Secure Remote Access (SRA) Series delivers enterprise-class device identification and interrogation features to small and medium-sized businesses. EPC for the SRA Series uniquely identifies Windows-based endpoints to tie them to authorized users. It also enforces granular security posture by checking for essential components such as anti-virus and anti-spyware software to ensure device integrity before admitting users of Windows-based devices via the Dell SonicWALL NetExtender client. The device interrogation list includes supported anti-virus, anti-spyware and personal firewall solutions from leading vendors such as McAfee®, Kaspersky Lab®, Symantec®, Computer Associates®, Sophos® and many others. This greatly reduces the chance of malware entering the network from non-IT-managed devices.

- **Easy, flexible device profiling**
- **Robust device identification**
- **Multiple device profile types**
- **NetExtender integration**
- **PC/desktop identification**

Features and benefits

Easy, flexible device profiling enables verification of the presence or absence of software on the endpoint device, including anti-virus, anti-spyware and personal firewall. It simplifies granular endpoint protection by allowing administrators to set up Windows device profiles from a comprehensive predefined list.

Robust device identification provides enterprise-class verification of endpoint criteria, such as domain membership and Windows version, as well as the presence of a client certificate on the endpoint.

Multiple device profile types include Allow and Deny with a customizable Deny message. If the endpoint matches a Deny device profile, the device user is presented with an appropriate message and is then allowed to remediate the device to fix its security posture. The device profiles can be enforced at the Global, User Group or User level.

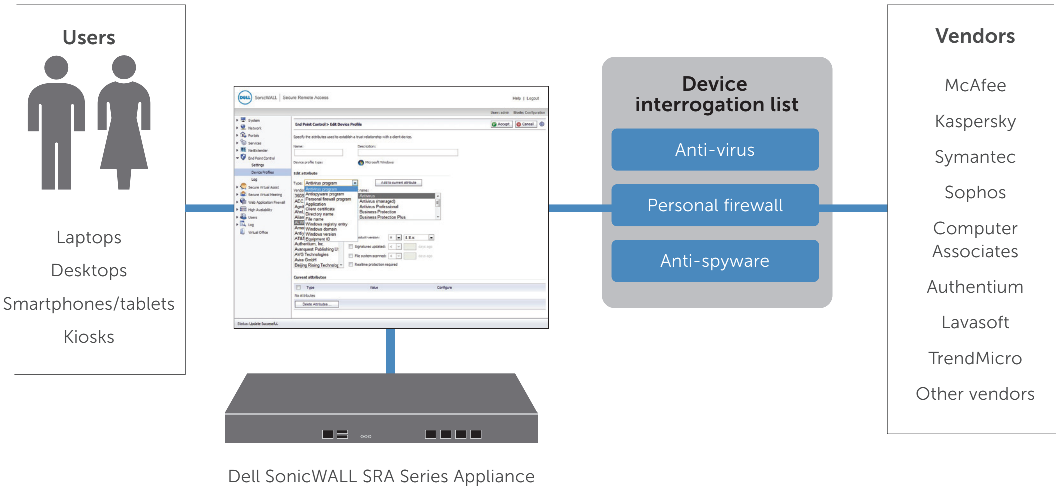
NetExtender integration allows dynamic provisioning of an EPC Dynamic Linked Library (DLL) to the endpoint device upon launching NetExtender, optimizing the client footprint on the device.

PC/desktop identification provides administrators with the ability to tie a Windows Device ID to a user by checking the device hard drive serial number via EPC interrogation and comparing this against information stored in Active Directory or LDAP. In addition, EPC for SRA Series identifies endpoints using additional criteria such as client certificates and domain membership.

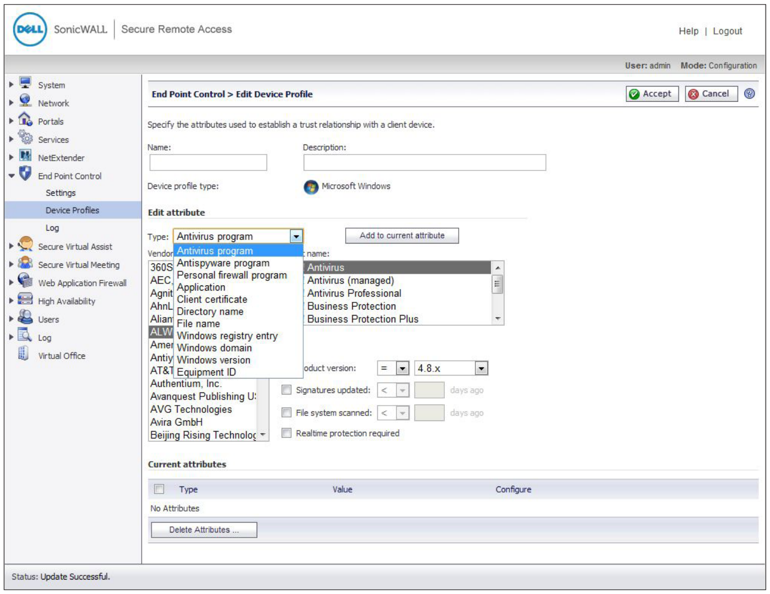
Granular endpoint policy criteria

EPC for SRA Series gives IT administrators the flexibility to confirm endpoint status based on:

- Windows domain membership
- Unique Windows device ID
- Registry keys and/or Windows patch levels
- Specific applications being run
- Anti-virus presence
- Anti-spyware presence
- Personal firewall presence
- Directory name
- Client certificate



EPC for SRA Series provides comprehensive, flexible device profiles that are easy to use and add. Administrators can select the specific vendor and product name for each solution category and can also specify which product version to check (e.g., the product must be version 7 or must be equal to or greater than version 6.x or must NOT be version 5). Administrators can also specify a date range in which the product last had its signature file updated (e.g., only allow access if the signature file was updated in the last 15 days).



User: admin Mode: Configuration

End Point Control > Edit Device Profile

Specify the attributes used to establish a trust relationship with a client device.

Name:

Description:

Device profile type: Microsoft Windows

Edit attribute

Type: Antivirus program

Vendor 360S, AEC, Agnit, AhnL, Alian, ALW, Amer, Antiy, AT&T, Authentium, Inc., Avanquest Publishing U:, AVG Technologies, Avira GmbH, Beijing Rising Technolog

name: Antivirus, Antivirus (managed), Antivirus Professional, Business Protection, Business Protection Plus

oduct version: = 4.8.x

□ Signatures updated: < days ago

□ File system scanned: < days ago

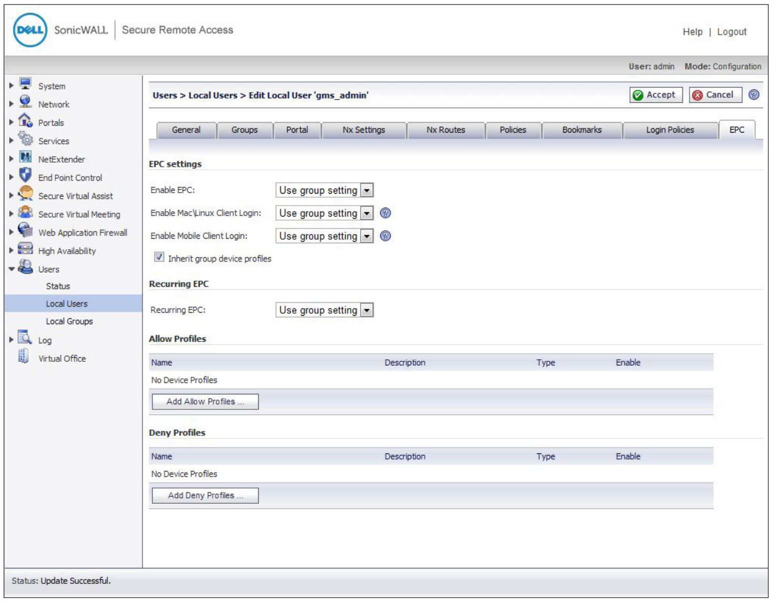
□ Realtime protection required

Current attributes

□ Type	Value	Configure
No Attributes		

Status: Update Successful.

Administrators can establish endpoint profiles based upon individual user and group criteria.



User: admin Mode: Configuration

Users > Local Users > Edit Local User 'gms_admin'

EPC settings

Enable EPC: Use group setting

Enable Mac\Linux Client Login: Use group setting

Enable Mobile Client Login: Use group setting

☑ Inherit group device profiles

Recurring EPC

Recurring EPC: Use group setting

Allow Profiles

Name	Description	Type	Enable
No Device Profiles			

Deny Profiles

Name	Description	Type	Enable
No Device Profiles			

Status: Update Successful.