Frequently Asked Questions

Secure Remote Access

Dell SonicWALL E-Class SRA Series FAQs

Contents

Frequently Asked Questions

1. What’s the difference between the E-Class SRA Series and a SRA 1600 or SRA 4600 model?

The main differences are performance, scale, policy control, and Management Interface workflows for policy administration. There are more subtle differences in access, and the E-Class SRA Series appliances differ in terms of license limits, not throughput. The E-Class SRA EX6000 and EX7000 models can be clustered in high availability pairs.

Policy Control

The E-Class SRA Series has very granular access control capabilities. Most rules control access is based on who the user is (the user’s name or group membership) and the destination resource. You can use other criteria in access control rules, such as the access method for a resource, the user’s network address, the zone of trust, or the date and time of the connection request.

Policy Administration

With all of this policy control, there is a comprehensive and sophisticated Management Interface that manages all the objects and workflow. The Management Interface for the SRA 1600 and 4600 is much more basic.

User Management

The E-Class SRA Series is user-centric. The base license is used to monitor and enforce concurrent user counts, and each of the E-Class SRA Series appliances has a different user count:

- Up to 250 users for the SRA EX6000
- Up to 5000 users for the SRA EX Virtual Appliance and SRA EX7000
- Up to 20000 users for the SRA EX9000

Depending on your licensing arrangements, however, you may be allowed to exceed the limit by a certain number of user sessions. By default, the appliance will allow the max license count to be exceeded by 10%. Once this occurs, the administrator is notified via Aventail Management Console (AMC) that more licenses are needed.

2. In what situations are a SRA 1600, SRA 4600, or E-Class SRA appliance appropriate?

Finding the right solution tends to involve some combination of these requirements:

- **Policy control** — If the customer needs a good deal of access control and customization for their users, then the E-Class SRA series appliances are the right choice.
- **End Point Control** — To protect sensitive data and ensure that your network is not compromised, a customer may want to make sure that the end point devices requesting access have certain attributes. With an E-Class SRA series appliance, you can set up profiles for devices to be tested against, and then classify them into zones (allow/deny/quarantine) based on the results.
- **Scale and/or high availability** — If a customer has more than 250 users, the E-Class SRA series must be used. With user counts lower than 250, it is the policy controls that matter. In general, the SMB market doesn’t need an E-Class SRA series appliance, the SRA 1600 or SRA 4600 is a better fit.

Most enterprises, however, must impose policy controls and have security requirements that only the E-Class SRA Series can meet.

3. What integration is there with GMS and what / when is more integration expected?

You can configure an E-Class SRA series appliance to be managed by the Global Management System (GMS). This includes basic system polling, uptime, and authenticated user reports, and the ability to launch the Aventail Management Console (AMC).

4. **How does the licensing work?**

   The E-Class SRA series is licensed based on concurrent users and is stackable. The appliance supports all access methods for up to that concurrent user count. The appliance also provides a small number of grace licenses above the user limit. The use of those licenses is logged as an early warning that some users might soon be denied access due to excessive user counts.

5. **Do the different access agents all consume a license?**

   Yes, each time the end user authenticates to the appliance, a license will be used. If the user logs in from two different devices, each device consumes a license. However, if the administrator deploys a web agent and a network agent to a single browser session, that session counts as only one license. Administrators can set limits on the number of active session a single user can maintain.

6. **Can the total number of concurrent users be partitioned in any way per realm?**

   No.

7. **Does Mobile Connect use a proxy-based or tunnel-based technology?**

   The technology is tunnel-based similar to the Connect Tunnel client.

8. **Is Mobile Connect available for a Blackberry mobile device?**

   Mobile Connect is not supported on a Blackberry, but users can access the web WorkPlace for browser based access to internal web sites from any device that has a SSL capable browser.

9. **Can the SSL timeout be disabled so mobile clients never have to re-authenticate?**

   No, however it can be configured to a large value, such as one week.

10. **Does Connect Tunnel use IPsec?**

    No, by default the Tunnel uses SSL (Port 443) but there is an option for increased performance in UDP heavy environments using ESP mode (UDP port 4500).

11. **Does the appliance support virtualization?**

    No, virtual routing and VLANs are NOT supported. However, you can configure up to 15 WorkPlace sites per appliance.

12. **What are the CPU and memory specifications?**

    SRA EX6000

    CPU: Intel Celeron 2.0 GHz

    RAM: 1 GB DDR533

    NIC: (4) PCIe GbE

    SRA EX7000

    CPU: Intel Core2 Duo 2.1 GHz

    RAM: 2 GB DDR533

    NIC: (6) PCIe GbE

    SRA EX9000

    CPU: Intel Quad Xeon 2.46 GHz

    RAM: 32 GB

    NIC: (4) 10 GbE SFP+, 8 1 GbE

13. **How is the performance under a heavy load of traffic?**

    The performance varies depending on the access agents used, and the types of applications being accessed. Translated Web access and the proxy mode clients are more CPU-intensive than Connect Tunnel or OnDemand Tunnel, which are both routed technologies.

14. **What operating system is the appliance based on?**

    The product is built on a custom version of Linux derived from Debian.

15. **Can I control the level of access granted to different user populations based on AD group membership?**

    Yes, authorization is supported against AD, LDAP, and RADIUS groups.

16. **What features are inclusive and which are licensed separately?**

    All appliances come with the base license including the Aventail Workplace Portal and the Aventail OnDemand Proxy/Tunnel agents. The SRA EX7000 and EX9000 are option-less with everything included. The SRA EX6000 and EX Virtual Appliance have optional add-ons which include Advanced End Point Control and Network Access Modules. See the datasheets for more details.

17. **Can the End Point Control engine verify that the latest Windows updates are installed?**

    No, not automatically, however you can create a device profile to check for the name of a file, registry entry, or a process running on the client device. Files can be checked by size, date, time, and integrity using hashes or the Windows Catalog.

18. **How are End Point Control library updates delivered?**

    Updates are delivered as part of a software upgrade or maintenance release. Dynamic updates are planned in a future release.

19. **My ACME AV application is not listed on the Advanced EPC menu. Can I still check for it some other way?**

    Yes, by identifying and searching for the running application or registry keys.

20. **Can the appliance detect it if I disable my AV client after connecting to the VPN?**

    Yes, by using the Persistent End Point Control checking feature.

21. **What's the time window in which Connect Tunnel can automatically re-establish after a network interruption?**

    20 seconds. Se the Administrator’s Guide for details.

22. **What port(s) need to be open on the external Firewall for client access to work?**

    Only port 443 needs to be open. Port 80 may also be opened and the appliance will redirect users to port 443. Also, if utilizing ESP mode then UDP port 4500 is also required.

23. **Can the WorkPlace portal be customized?**

    Yes, within the Management Console, the logo, title, colors, help text, End User Acceptance Agreement, and layouts can all be customized. Additional customization can be performing by creating a WorkPlace template which is described in the Admin Guide.

24. **Can different Realms reference the same authentication server?**

    Yes.

25. **Is it possible to provide unauthenticated access to some resources?**

    Yes, using a null authentication Realm.

26. Will my custom Web application work through the WorkPlace portal?

Yes, using either the Translated or Virtual Hosts mode for pure reverse proxy access or the Web Proxy Agent your custom application should work normally.

27. How do I generate usage reports?

Use the Dell SonicWALL Advanced Reporting option.

28. Can I migrate the configuration from one appliance to another?

Yes, configuration files are transportable between appliances. Note that importing a configuration from a newer release to an older release is not supported.

29. Is there a charge for software upgrades?

No, it's included with the annual maintenance.

30. Does the appliance use a hard disk?

Yes.

31. Can you run two appliances in HA mode if they are not co-located?

No, this configuration is not supported.

32. Is it possible to spread the “cluster” across physical locations? For example, rather than use a crossover cable, can we run this through a switch and have both systems be in different physical locations.

It is not a supported configuration.

33. Will the access agents activate if ActiveX is blocked?

The appliance attempts to use Java if ActiveX is blocked or disabled, but this depends on the specific circumstances.

34. Can Aventail Access Manager be pre-installed by an administrator outside the VPN context?

Yes, a separate installation package is available for all endpoint components.

35. Does Aventail Access Manager require local administrator rights?

No.

36. Does Aventail Secure Virtual Desktop require local administrator rights?

No.

37. How can I configure the appliance remotely if the Aventail Management Console is not reachable via the external interface?

Connect via the VPN and configure the AMC URL as a permitted resource.

38. When upgrading a cluster, what is the best procedure? Which node should be upgraded first?

It is best to upgrade the master node first. As the upgrade starts, traffic flows to the secondary system. When the upgrade is complete and the master node comes back online, it will notice that the slave node's version differs from its own. It stops the services on the slave node and services all incoming requests itself. You can then install your upgrade on the slave node in AMC. More information on this can be found in the *Installation Guide* and *Administrator's Guide*.

39. Can I export my configuration from a system and import it into a different system, such as from an SRA EX6000 to an SRA EX7000?

Yes, a full import is possible from one appliance to another. Another option is a partial import which will contain only the policy portion of the configuration such as Realms, Resources, ACLs, and EPC configuration, and not node or hardware specific information.

40. What is the difference between Connect Tunnel and OnDemand Tunnel? Is there anything I cannot do in one that I can do in the other?

Both OnDemand and Connect are tunneling technologies that actually share the same code. They differ in terms of how they are installed and activated:

- Connect Tunnel is installed on the desktop, it shows up as a Network Interface and has a System Tray icon for configuration.
- OnDemand Tunnel is automatically provisioned and activated via the WorkPlace Portal, and is just a temporary network adapter that can only be initiated by the WorkPlace.

Since Connect Tunnel is an installed agent it can also be used for pre-domain login processing. When the computer starts up, you can use **Ctrl-Alt-Delete** and select **Logon Using…**, Connect Tunnel will show up as an adaptor, which allows such things as logon scripts to run. This is not possible with OnDemand because the user has already logged on to the computer. Connect Tunnel also supports fallback (in case a primary appliance becomes unavailable) and suspend/resume.

41. When I set up administrator accounts is it possible to point to an external authentication repository like our Active Directory server?

Yes, any authentication method that is supported on the appliance can be required for strong authentication to administrative accounts.

42. What are the maximum TCP connections that SRA EX6000 and SRA EX7000 can support?

Connections to the appliance are measured in terms of concurrent users, not TCP connections. For the SRA EX6000 and SRA EX7000, the maximum concurrent users supported are 250 and 5000 per unit, respectively.

43. Can I activate a Spike License and use it periodically, a few days at a time, until I use up the specified number of days?

Yes, a Spike License can be used as many times as necessary within a 10 or 30 day total period.

44. Do you support native RSA ACE natively?

Yes, RSA Authentication Manager is supported natively. The RADIUS protocol can also be used to connect to a RSA server.

45. Can the appliance prohibit multiple same-user logins?

Yes, the administrator can control the maximum number of active session per user on a Community basis.

46. How do I upgrade my licensed user count?

A customer must purchase a user upgrade license, enter the provided activation key in MySonicWALL, retrieve the updated license from MySonicWALL, and apply the updated license to the appliance.

47. How does an HA pair of appliances work: active/active or active/passive?

Currently, only an active/active implementation is supported.

48. Can I replicate a policy between appliances in real time?

No. With our policy replication feature, one appliance (it can be any appliance in the "collection" or replication pool) acts as the policy master where all policy editing is done. Policy can then be pushed out from the policy master to the other appliances in the collection by the administrator.

49. How many WorkPlace sites am I allowed to create?

We support a maximum of 15 WorkPlace sites per appliance/HA-pair.

50. Can I program Connect Tunnel to operate behind the scenes with my application?

Yes, the ngdial command line tool is used by several partners. We also have some customers that use the Microsoft RAS APIs to automate connections.

51. Can you work behind an external load balancer?

Yes, we are certified with RadWare and work with various F5 and Cisco configurations; many of our customers use external load balancers.

52. Can I customize Connect Tunnel’s appearance?

Yes, you can customize the text that appears for the Connect Tunnel client in the user interface.

53. How can I install Connect Tunnel if I don’t have administrator rights?

You cannot install Connect Tunnel if you do not have administrator rights. For this reason our customers typically use a software distribution system like Microsoft’s SMS to image their corporate laptops with Connect Tunnel. Once it is installed, it can be updated without administrator rights.

54. How do I get Connect Tunnel Service to run with my application?

In a server environment, you can install and configure the Connect Tunnel Service so that the VPN connection starts automatically using a pre-assigned username & password. The connection can then be scheduled using the Windows Scheduler and is established without user intervention, and no user interface or icons are displayed. All applications on the system can use it for access to the remote network.

55. Can I reserve licenses for upper management or IT staff?

No, licenses are allocated on a first-come first-serve basis.

56. Can I deliver Connect Tunnel via SMS?

Yes, we provide an MSI package for this purpose.

57. Does the client software automatically update itself on the client machines?

Web based client components such as the Web Proxy Agent, OnDemand, and the Native Access Modules are updated automatically on the end point upon connection to the appliance after a hot fix, maintenance release, or upgrade has been performed on the appliance. The Connect Tunnel client can be configured to allow users to defer the update for 24hrs before being prompted again, to notify the users and force the update, or to simply force the update without notifying the user.

58. How do I get notified when updates or new releases are available?

You can log in to MySonicWALL.com to check for updates, as well as sign up for various alerts through the SonicWALL Knowledge Portal. We are considering enhancing Aventail Management Console to notify administrators when they become available.

59. Are you FIPS compliant?

Yes.

60. If I am at my license count limit what happens to the next user who tries to log in?

It depends on whether you have exceeded the grace count. Once the grace limit is reached, it refuses to log in new users and notifies them that the system is at maximum capacity.

61. Can you detect incoming viruses and stop them?

No, that is the function of a Dell SonicWALL Next Generation Firewall. We do however have the ability to enforce that an approved AV, PFW, or ASPY client is installed, running, and up to date on the end point using Aventail's End Point Control capabilities. Clients which do not meet the defined criteria can be denied access or placed into a Quarantine Zone where they can be given the opportunity to remediate their devices.

62. Do you support the Mac OS X and iOS?

Yes.

63. Does Aventail Secure Virtual Desktop run on Mac?

No, only the Windows operating system is supported.

64. Can I change my domain password? Does it notify me when a password is about to expire?

Yes and yes. The ability for a user to change their password requires a secure connection (SSL) between the authentication server and the Aventail appliance, however this is not required for simply notifying the user that their password is due to expire. See the *Administrator’s Guide* for more details.

65. Does it support NAC/NAP?

The End Point Control (EPC) feature provides a similar function in that endpoints are checked for compliance before a VPN session is established. Based on the results of the EPC compliance check, endpoints can be allowed access, allowed limited access, placed into a Quarantine Zone, or denied access.

66. Can I set up different types of access based on who users are or what sort of devices they are using?

Yes.

67. Can multiple WorkPlace portals be configured using the same appliance?

Yes.

68. What operating systems support Aventail Secure Virtual Desktop?

Operating System	Web Browser	Notes
• Windows 8 32-bit and 64-bit	• Internet Explorer 10.0 32-bit only • Firefox 18.0	• ActiveX • Java 1.7.0 update 11 • Java 1.6.0 update 37 or earlier When not using ActiveX on Windows, Sun/Oracle JRE 1.6 or later is required. JRE 1.7 is recommended.
• Windows 7 SP1 32-bit and 64-bit • Windows 7 32-bit and 64-bit • Windows Vista SP2 32-bit and 64-bit • Windows XP Pro SP3	• Internet Explorer 10.0 32-bit only • Internet Explorer 9.0 32-bit only • Internet Explorer 8.0 32-bit only • Firefox 18.0	• ActiveX • Java 1.7.0 update 11 • Java 1.6.0 update 37 or earlier When not using ActiveX on Windows, Sun/Oracle JRE 1.6 or later is required. JRE 1.7 is recommended.
• Mac OS X 10.8 64-bit • Mac OS X 10.7 32-bit and 64-bit • Mac OS X 10.6 32-bit and 64-bit	• Safari 6.0 • Safari 5.1 • Safari 5.0	• Mac OS X support is based on Apple policy of the 2 most recent releases as fully supported.
• Linux kernel 2.4.20 or later 32-bit and 64-bit	• Firefox 18.0	

69. What is a Spike License?

A Spike License enables you to handle a temporary spike in the number of users who are being given secure remote access to resources. For example, in the event of a natural disaster, you might have a jump in the number of employees who need to access resources from home. The Spike License is valid for a limited amount of time, which begins when it is activated and used.

70. Can the E-Class SRA series appliance be deployed in two-arm mode?

Yes, that is the recommended mode.

71. What is the Native Access Module?

The Native Access Module provides for integrated web based access from the WorkPlace Portal to Windows Terminal Server (RDP), Citrix (ICA), VMware View, Telnet, and SSH applications.

72. Does the E-Class SRA series appliance have a LiveMeeting add-on?

No.

73. Does the E-Class SRA series appliance have a remote assistance add-on?

Yes, the Virtual Assist feature is available on all appliances.

74. How can I use device watermarks and the End Point Control feature to identify whether an endpoint is trusted?

Device ID is supported on all platforms which allows a hardware identifier to be stored and tied to a specific user. When the user connects, the Device ID is checked against the stored value to assure that the user is connecting from a “trusted” endpoint.

75. Must I purchase three certificates to be installed on the E-Class SRA series appliance?

Customers are not required to purchase any certificates. The appliance provides the ability to create self-signed certificates for the purposes of evaluation or casual use of the remote access appliance, however, commercial certificates issued by a trusted Certificate Authority are highly recommended for production deployments as they offer a higher degree of security and protection against man-in-the-middle attacks.

76. Are there self-signing certificates available in the E-Class SRA appliance?

Yes.

77. If I have configuration problems on the E-Class SRA series appliance, can I reset it as I would with other Dell SonicWALL appliances?

Yes, you can roll back hotfixes, roll back to the previous firmware version, or reset the appliance to factory defaults.

78. For device watermarking, can we use a hash algorithm to collect and transform the end point hardware information and use the hardware hash output as part of the CSR of the device?

You do not need to. For a certificate to be valid and verified, it must have its private key in the client key chain.

79. Can a username and password be tied to a digital certificate?

Yes, multiple stacked authentication methods are supported.

80. How do you separate communities of users with 802.1q VLAN-tagging for the Connect Tunnel feature or for bookmarks?

We do not currently support 802.1q VLAN tagging and require 802.3 framing on our interfaces.

81. How can users find out why they are in the untrusted zone?

For security reasons, this information is not available to the end users, just the system administrator. Administrators have the option of configuring remediation or quarantine zones to inform the user what components need to be corrected.

82. You have device watermarking...that’s great! But I don’t have CA and certificate implementation is complex. Can we limit user access some other way?

Our recommendation is for administrators to place files on endpoint devices that are part of a device profile, along with a hash for verifying that the file is legitimate. They can also enumerate a series of files/directories/processes that are known to be present on managed or corporate issued devices. In addition, customers can use their own certificate authority to generate client certificates.

83. Can the E-Class SRA series appliance scan for viruses?

No, our strategy is to integrate with our Dell SonicWALL Next Generation Firewall products.

84. Can your product pre-scan user computers for malware? How is the scanning pattern database updated?

No, but with End Point Control you can check if a required endpoint security product is installed and running before a VPN connection is permitted.

85. Can the E-Class SRA series appliance execute a user’s domain login script automatically to perform tasks like drive mapping?

Yes, Connect Tunnel provides the ability to leverage the domain login script when used as a dial-up adapter at the time of login to the Windows device. It is also possible to launch scripts or executables either on the end-point or on a UNC path (after the initial VPN login) by using the "post-connection scripting" feature configurable for both Connect Tunnel and OnDemand Tunnel connections**.**

86. **With Aventail Cache Cleaner and Aventail Secure Desktop, users sometimes see an error message about Java missing.**

    Both components require Java. A current version of Java must be installed before use.

87. **What sort of log information do you collect?**

    The system message log displays server processing and diagnostic information about the network tunnel service and the Web proxy service. It also provides detailed messages regarding all access control decisions e.g. each time a user request matches a policy rule, or when a log file entry is recorded explaining the action taken. There are two access service audit logs: one for the Web proxy service, and one for network tunnel services. They provide detailed information about connection activity, including a list of users and the amount of data transferred.

88. **Can the E-Class SRA series appliance log show the user login time and logout time for WorkPlace and tunnel agents?**

    Yes.

89. **Do you have a reference table for E-Class SRA series appliance error codes?**

    No, we do not have a reference table documented. In 10.0, we provide much-improved troubleshooting that uses a database with searchable tags. For most issues this will eliminate the need to sift through the log files, which will improve the customer experience and help our support organization.

90. **Does this product support local password management by users in a local authentication database?**

    Yes.

91. **Does this product support virtualization?**

    Not at the network level. We have segmented the system at the policy level and at the WorkPlace portal service level. We support delegated administration so subsidiaries and departments can administer their own resources. We also provide virtualization of WorkPlace sites that have their own VIPs, style sheets with ornamentation, resource visibility, and resource access control. This type of virtualization is aimed at enterprises with their own on-premise appliances, as opposed to hosted service providers, who need network segmentation.

92. **Can you limit the number of user logins at each WorkPlace site?**

    Yes, an administrator can limit the number of logins a user can have.

93. **Do you support a web-based, built-in email client for the IMAP and POP3 protocols?**

    No, nor are there any plans to do so.

94. **Do you have a Chinese user interface?**

    Yes, we do have localization available for Chinese.

95. **Do you support multiple site clusters for our data redundancy solution?**

    No, administrators can use third-party global load balancers such as F5, Cisco and RadWare. We have several customer sites that have deployed this configuration.

96. What Smartphones/Tablets are supported?

Support is provided for web access from any SSL capable browser. Tunnel access is provided using Connect Mobile for iOS and Android devices.

97. What is the difference between using one or two interfaces?

Customers who prefer to use a dual-arm, classic DMZ with external and internal firewalls should configure the appliance for dual interface mode. Sites that use the Cisco single-arm model should use the single interface model. We recommend the dual interface model because it is more secure and our systems scale better using two interfaces. HA clustering of tunnel service works only in dual interface mode.

Last updated: 9/3/2013