



**Juniper Networks Secure Access**

**Secure Virtual Workspace**

*Release 5.3R3*

**Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

**[www.juniper.net](http://www.juniper.net)**

Part Number: 53B050606

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986–1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.BSD and 4.BSD-Lite Releases is copyrighted by The Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, The Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, E-series, ESP, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, T-series, and TX Matrix. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Copyright © 2006, Juniper Networks, Inc.  
All rights reserved. Printed in USA.

*Juniper Networks Secure Access Administration Guide*, Release 5.3

Writer: Mark Smallwood

Editor: Claudette Hobbart

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

#### Year 2000 Notice

Juniper Networks hardware and software products are Year 2000 compliant. The JUNOS software has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at [www.juniper.net/techpubs](http://www.juniper.net/techpubs).

#### End User License Agreement

**READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE.** BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

**1. The Parties.** The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

**2. The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller.

**3. License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use the Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller, unless the applicable Juniper documentation expressly permits installation on non-Juniper equipment.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

**4. Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Software on non-Juniper equipment where the Juniper documentation does not expressly permit installation on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; or (k) use the Software in any manner other than as expressly provided herein.

**5. Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

**6. Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

**7. Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

**8. Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

**9. Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

**10. Taxes.** All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

**11. Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

**12. Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

**13. Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

**14. Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

**15. Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language).)



# Secure Virtual Workspace

The Secure Virtual Workspace (SVW) provides a protected desktop for Windows XP and Windows 2000 users. You can create an SVW policy when you configure your Host Checker policies, as described in the following topics:

- “Enabling the Secure Virtual Workspace” on page 200
- “Secure Virtual Workspace features” on page 200
- “Secure Virtual Workspace restrictions and defaults” on page 201
- “Configure the Secure Virtual Workspace” on page 202
- “Define Secure Virtual Workspace permissions” on page 202
- “Define a Secure Virtual Workspace application policy” on page 203
- “Define a Secure Virtual Workspace security policy” on page 204
- “Define Secure Virtual Workspace environment options” on page 205
- “Define Secure Virtual Workspace remediation policy” on page 205

---

## Enabling the Secure Virtual Workspace

The Secure Virtual Workspace guarantees the integrity of IVE session data on a client machine running Windows 2000 or Windows XP by creating a protected workspace on the client desktop. By enabling the Secure Virtual Workspace, you ensure that any end-user signing in to your intranet must perform all interactions within a completely protected environment. If the user's applications and interactions result in data being written to disk or to the registry, the Secure Virtual Workspace encrypts that information. When the IVE session is complete, the Secure Virtual Workspace destroys all information pertaining to itself or to the session, by default. However, you can configure the state of this type of information to suit your particular needs. For example, you might decide to allow data to persist across Secure Virtual Workspace sessions.

The IVE follows the DoD 5220.M cleaning and sanitization standard for securely deleting Secure Virtual Workspace data that is stored on the hard disk.

The Secure Virtual Workspace:

- Removes workspace data and resources when the session ends.
- Ensures that no browser Helper Objects latch onto an Internet Explorer process before launching IE.
- Prohibits desktop search products from intercepting Web traffic and indexing the contents.
- Enters all of its configuration and run-time operations in IVE logs.

The IVE hosts the Secure Virtual Workspace binary, which the client system downloads from the IVE whenever a user connects. The Secure Virtual Workspace creates a virtual file system and a virtual registry on the client.

You define and configure the applications that are allowed to run within the Secure Virtual Workspace. For example, you can configure the following types of application configurations:

- Restrict launching of Internet Explorer and Outlook to the Secure Virtual Workspace.
- Restrict application installations and executions within a Secure Virtual Workspace session. This ensures that even the application binaries are completely removed from the client machine after the session ends.

### **Secure Virtual Workspace features**

The IVE implementation of the Secure Virtual Workspace:

- Does not require the client desktop user to have administrator privileges to download and run the Secure Virtual Workspace.

- Supports the use of the Secure Virtual Workspace in conjunction with Host Checker, which will automatically launch in the secure workspace, when initiated.
- Provides the Secure Virtual Workspace as a J.E.D.I. module, to allow you to create Secure Virtual Workspace policies in Host Checker.

### **Secure Virtual Workspace restrictions and defaults**

The Secure Virtual Workspace imposes certain restrictions on its use, and establishes defaults, which you may be able to modify.

- By default, a platform-specific browser is allowed to run in the SVW, unless explicitly restricted by the administrator.
- The IVE does not allow software applications that update the HKLM registry entries on installation to operate within the SVW.
- The IVE does not support the standard J-SAM applications Outlook and Netbios file browsing through SVW, since these applications require registry key changes. However, the IVE does support the Citrix and Lotus Notes J-SAM standard applications through SVW.
- By default, the IVE does not allow access to external storage and printing devices by some applications running in SVW. You can enable access to these devices in the SVW policy, if needed.
- By default, end-users are unable to access network shares, unless you configure access to network shares in the SVW policy.
- If your end-users use firewalls or other applications that run in the kernel space, they may experience problems when trying to download IVE client components in SVW. Low-level administrative applications may display message boxes requiring user interaction. If you set the option to allow switching to the default or real desktop, the user may be able to dismiss the message boxes. If the switching option is disabled, users may be unable to fix the problem.
- SVW does not support 16-bit applications.
- Some Windows keyboard shortcuts may not work properly inside an SVW session.
- To display the Windows Task Manager while in SVW, you cannot use the standard keyboard shortcut Ctrl + Alt + Del. You must right-click on the Windows taskbar (typically on the bottom of the screen, unless you have moved it) to display a popup menu, from which you can select **Task Manager**.
- If you set the Host Checker status update interval to a value of zero (0), Host Checker will perform the status check once and then quit. If Host Checker quits, SVW also quits. As a result, the end-user is unable to initiate an SVW session. Set the Host Checker status update interval to a non-zero value.

## Configure the Secure Virtual Workspace

You configure the Secure Virtual Workspace within the context of a Host Checker policy and all Secure Virtual Workspace policies you define appear in a list at **Authentication > Endpoint Security > Host Checker**.



**NOTE:** Because the Secure Virtual Workspace session data is stored on the end-user's real desktop, you should implement the persistence feature only if each of your end-users always uses the same client machine.



**NOTE:** No provision has been made to ensure that you cannot configure a sign-in URL mapping to more than one realm configured with an SVW policy. If you configure multiple mappings to more than one realm, the results are unpredictable. You must explicitly configure the secure virtual desktop to allow only one SVW policy to be evaluated at the user end.

### Define Secure Virtual Workspace permissions

You can specify which devices and resources the end-user can access when using the Secure Virtual Workspace.

To define a new Secure Virtual Workspace permissions policy:

1. In the Web console, choose **Authentication > Endpoint Security > Host Checker**.
2. Under **Policies**, click **New Secure Virtual Workspace Policy**.
3. Under **Permissions**, check the appropriate checkboxes for the items to which you want to grant permissions:
  - **Printers**—Select to allow end-user access to network printers.
  - **Restricted View of Files**—When Restricted View is set, only the directories Documents and Settings, Program Files, and the Windows system folders on the system drive (typically c:) are available within SVW.



**NOTE:** If you set the **Restricted View of Files** option, and your end-users configure partitioned drives, they will be unable to access any applications or files residing on any drive other than the system (c:) drive. If you allow your end-users to partition drives, you should not use the Restricted View.

- **Removable Drives**—Select to allow end-user access to removable drives on the end-user's client machine.

If an end-user installs a USB removable storage device he may experience the two following behaviors, depending also on how you set this option:

- If the user connects the USB device after initiating an SVW session, the device will appear to be a fixed hard drive and the user will not be able to read or write to the device during an SVW session, even when you have set the **Removable Drives** option.
  - If the user connects the USB device before initiating an SVW session, the device appears to be removable media and the user can access it, if you have set the **Removable Drives** option when configuring SVW.
  - **Network Share Access**—Select to allow end-user access to network share drives.
  - **Switch to Real Desktop**—Select to allow end-user to toggle between the Secure Virtual Workspace and the end-user’s client desktop.
  - **Desktop Persistence**—Select to allow end-users to maintain a Secure Virtual Workspace across client sessions on NTFS file systems only. Desktop persistence is not supported on FAT16 or FAT32 file systems.
4. Continue to define the policy or click **Save Changes**.

### Define a Secure Virtual Workspace application policy

You can specify which applications the end-user can install or run when using the Secure Virtual Workspace.

To define a new Secure Virtual Workspace application policy:

1. In the Web console, choose **Authentication > Endpoint Security > Host Checker**.
2. Under **Policies**, click **New Secure Virtual Workspace Policy** or click the hyperlinked name of an existing Secure Virtual Workspace policy.
3. Under **Applications**, select the checkboxes for the types of applications you want to enable:
  - **Control panel**—Select to allow the end-user to access the Windows control panel while in the Secure Virtual Workspace.
  - **Run menu**—Select to allow the end-user to access the Windows run menu while in the Secure Virtual Workspace.
  - **Registry editor**—Select to allow the end-user to access the Windows registry editor (regedt32.exe) while in the Secure Virtual Workspace.
  - **Task manager**—Select to allow the end-user to access the Windows Task Manager (taskmgr.exe) and system processes while in the Secure Virtual Workspace.
  - **Command window**—Select to allow the end-user to access the Windows Command window (cmd.exe) and execute commands while in the Secure Virtual Workspace.

- **Custom applications**—You can identify custom applications that the end-user is allowed to run while in the Secure Virtual Workspace. For example, you might include in-house applications, non-default browsers, and other types of applications. Enter one application, including the `.exe` extension per line in the multiline text box. You can also use the `*` wildcard for an entire class of applications, and you can include an optional MD5 hash value following the executable name and a comma, for example, `telnet.exe,0414ea8`.
- **Applications to deny**—You can identify applications you want to restrict from end-user use while in the Secure Virtual Workspace. Enter one application, including the extension for each executable per line in the multiline text box.

**NOTE:**

- Any custom application that is not listed in the Custom applications field is denied by default.
  - If you add the same application to the **Custom applications** text box and to the **Applications to deny** text box, the deny action takes precedence and users will be denied access to the application SVW sessions. Be aware that this can happen if you use wildcards to specify applications in both lists. For example, if you specify `*plore.exe` in the allow list and `ie*.exe` in the deny list, then `ieexplore.exe` will be denied.
- 

4. Continue to define the policy or click **Save Changes**.

After you define one or more Virtual Workspace policies, you must enable them as Realm authentication policies at the user level, as described in “Implementing Host Checker policies” on page 240.

### Define a Secure Virtual Workspace security policy

You can specify encryption levels and can control the use of 3rd-party extensions in Internet Explorer and Outlook.

To specify security options for a new Secure Virtual Workspace policy:

1. In the Web console, choose **Authentication > Endpoint Security > Host Checker**.
2. Under **Policies**, click **New Secure Virtual Workspace Policy** or click the hyperlinked name of an existing Secure Virtual Workspace policy.
3. Specify the type of **AES** encryption key the IVE uses to enable the Secure Virtual Workspace on the client. The available options are 128, 192, and 256-byte encryption keys.
4. Identify the IE or Outlook extensions you want to allow by including each allowable DLL on a separate line in the **IE/Outlook extensions to allow** text box. Any extension that is not listed is denied, by default.

These extensions are small applications that are passed into and out of the Secure Virtual Workspace session.

5. Continue to define the policy or click **Save Changes**.

### Define Secure Virtual Workspace environment options

To specify environment options for a new Secure Virtual Workspace policy:

1. In the Web console, choose **Authentication > Endpoint Security > Host Checker**.
2. Under **Policies**, click **New Secure Virtual Workspace Policy** or click the hyperlinked name of an existing Secure Virtual Workspace policy.
3. Under **Options**, specify the maximum length of time (in minutes) a client's Secure Virtual Workspace session can remain idle before the connection to the IVE times out.
4. Specify the desktop wallpaper image (Optional).
5. Specify the desktop background color (Optional).
6. Specify the sign-in URL to use to access the SVW.

The available URLs include the default User sign-in URL and any URLs you have defined in **Authentication > Signing in > Sign-in Policies**. The first time SVW puts the user into the virtual workspace and initiates a browser, it takes the user to the IVE using a sign-in URL. By default, this sign-in URL is the same one that the user has entered to start their IVE session. You can configure a different sign-in URL through this option.

7. Continue to define the policy or click **Save Changes**.

### Define Secure Virtual Workspace remediation policy

To specify remediation options for a new Virtual Workspace policy:

1. In the Web console, choose **Authentication > Endpoint Security > Host Checker**.
2. Under **Policies**, click **New Secure Virtual Workspace Policy** or click the hyperlinked name of an existing Secure Virtual Workspace policy.
3. Under **Remediation**, select remediation options for users whose computers do not meet the requirements specified in the policy. For instructions, see "Configure Host Checker remediation" on page 248.



**NOTE:** If you do not create remediation instructions and the policy fails, your users will not know why they cannot launch the Secure Virtual Workspace or access local resources.

---

- **Enable Custom Instructions**—Select to expand text box in which you can enter custom instructions, using either text or HTML, that will be presented to end-users when the Secure Virtual Workspace encounters a remediation problem.
- **Evaluate Other Policies**—Select to open list boxes that allow you to choose other existing Host Checker policies to be evaluated when initiating the Secure Virtual Workspace.
- **Remediate**—Select to apply remediation rules.
- **Kill Processes**—Select to open text box in which you enter application processes and MD5 hash values for the processes you want killed. For example:  
  
Application.exe  
MD5: 6A7DFAF12C3183B56C44E89B12DBEF56  
MD5: 9S3AJ912CC3183B56C44E89B12DI2AC9
- **Delete Files**—Select to open text box in which you can enter file names, one per line, of files you want deleted.

4. Click **Save Changes**.