Configuration

User Guide

Version R95

English

July 20, 2017

Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contents

Configuring the Server

The server is the heart of the system. Users access all functions through this server's web interface. The agents, on all managed machines, connect to this server to get any instructions/tasking orders. Your server must be accessible to both users and agents.

For configuring the server, see the latest **installation instructions** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/install/index.asp#home.htm)*.

System Security

We designed the system with comprehensive security throughout. Our design team brings over 50 years of experience designing secure systems for government and commercial applications. We applied this experience to uniquely combine ease of use with high security.

The platform's architecture is central to providing maximum security. The agent initiates all communications back to the server. Since the agent will *not* accept any inbound connections, it is virtually impossible for a third party application to attack the agent from the network. *The system does not need any input ports opened* on the managed machines. This lets the agent do its job in virtually any network configuration without introducing any susceptibility to inbound port probes or new network attacks. VSA also creates a **certificate to authenticate agents** *(https://helpdesk.kaseya.com/entries/101529308)*.

The VSA protects against man-in-the-middle attacks by encrypting all communications between the agent and server with AES 256 using a key that rolls every time the server tasks the agent. Typically at least once per day. Since there are no plain-text data packets passing over the network, there is nothing available for an attacker to exploit.

Users access the VSA through a web interface after a secure logon process. The system never sends passwords over the network and never stores them in the database. Only each user knows his or her password. The client side combines the password with a random challenge, issued by the VSA server for each session, and hashes it with SHA-256. The server side tests this result to grant access or not. The unique random challenge protects against a man-in-the-middle attack sniffing the network, capturing the random bits, and using them later to access the VSA.

Kaseya uses TLS for all secured HTTP and WebSocket connections. See the following security related topics for more information:

- Using Security Certificates
- Importing a Security Certificate
- Automatically redirect to https at logon page

Minimum System Requirements

See up to date **minimum system requirements** *(http://help.kaseya.com/WebHelp/EN/VSA/9050000/reqs/index.asp#home.htm)*.

Updating or Moving the VSA

If you are updating from an earlier version of Kaseya to this version, or want to update or move your existing K2 server to the latest version, see the latest **installation instructions**

(http://help.kaseya.com/webhelp/EN/VSA/9050000/Install/index.asp#home.htm).

Logon and Browser Settings

To logon to Virtual System Administrator™

1. Use your browser to display the logon page of your VSA server.
2. Enter your user name and password.

   Note: For initial logon, use the master user account name and password entered during installation.

3. Check the **Remember my username and domain (if any) on this computer** checkbox to save the username and domain name to a cookie on the local computer so you don't have to re-enter each time you log in. The password is not stored.

   Note: The **Discovery** add-on module can be used to manage VSA user logons and Portal Access logons using **domain logons** *(http://help.kaseya.com/webhelp/EN/KDIS/9050000/index.asp#7293.htm).*

4. Click the **Logon** button.

Note: To prevent unauthorized access after making configuration changes, log off or close the session by terminating the browser application.

Enabling Browser Cookies, JavaScript and Popups

Your browser must have cookies and JavaScript enabled in order to proceed. Popups for the VSA website are recommended.

Internet Explorer

To Enable Cookies in Internet Explorer 10, 11

1. Click the **Tools** menu or gear icon.
2. Select **Internet Options**.
3. Switch to the **Privacy** tab.
4. Select a privacy setting no greater than **Medium High** (i.e. the setting must not be High nor Block All Cookies).
5. Click **OK**.

To Enable JavaScript in Internet Explorer 10, 11

1. Click on the **Tools** menu.
2. Select **Internet Options**.
3. Switch to the **Security** tab.
4. Click on **Internet** in the **Select a Web** content zone.
5. Press the **Custom level...** button.
6. Scroll down to the **Scripting** section.
7. In **Scripting of Java applets**, click the **Enable** option.
8. Click **OK**.

To Enable Popups in Internet Explorer 10, 11

1. Click the **Tools** menu.

2. Select **Internet Options**.
3. Switch to the **Privacy** tab.
4. Click **Settings**. The **Pop-up Blocker Settings** dialog displays.
5. Enter the URL or IP address of your VSA in the **Address of website to allow** field.
6. Click **Close**, then **OK**.

Firefox

To Enable Cookies in Firefox

1. Click the **Firefox** menu.
2. Select **Options**.
3. Switch to **Privacy** settings.
4. Set History to **Remember History**. (You can also **Use custom settings for history** and make sure **Accept cookies from site** is checked.)
5. Click **OK**.

To Enable JavaScript in Firefox

1. Click the **Firefox** menu.
2. Click **Addons**.
3. Click **Plugins**.
4. Click the **Java** plugin to select it.
5. Select the **Always Activate** option.

To Enable Popups in Firefox

1. Click on the **Firefox** menu.
2. Select **Options**.
3. Switch to the **Content** tab.
4. Click **Exceptions...** The **Allowed Sights - Pop-ups** dialog displays.
5. Enter the URL or IP address of your VSA in the **Address of web site** field.
6. Click **Allow**.
7. Click **Close**, then **OK**.

Chrome

To Enable Cookies in Chrome

1. Click the **Wrench** icon.
2. Select **Settings**.
3. Click **Show advanced settings**.
4. In the **Privacy** section, click **Content settings**.
5. Select the **Allow local data to be set (recommended)** option.
6. Click **OK**, then **Close** for all the parent dialogs.

To Enable JavaScript in Chrome

1. Click the **Wrench** icon.
2. Select **Settings**.
3. Click **Show advanced settings**.

4. In the **Privacy** section, click **Content settings**.
5. Select the **JavaScript** feature.
6. Select the **Allow all site sites to run JavaScript (recommended)** option.
7. Click **OK**, then **Close** for all the parent dialogs.

To Enable Popups in Chrome

1. Click the **Wrench** icon.
2. Select **Settings**.
3. Click **Show advanced settings**.
4. In the **Privacy** section, click **Content settings**.
5. Select the **Pop-ups** feature. (You may have to scroll down to see it.)
6. Select the **Do not allow any site sites to show pop-ups (recommended)** option.
7. Click **Manage Exceptions...** The **Pop-up Exceptions** dialog displays.
8. In the **Add new hostname pattern edit box** at the bottom of the list, enter the URL or IP address of your VSA.
9. Set **Action** to `Allow`.
10. Click **OK**, then **Close** for all the parent dialogs.

Index