



Hewlett Packard
Enterprise

HPE Remote Device Access

RDA Install Guide

Legal Notices

Remote Device Access

© Copyright 2015-2025 Hewlett Packard Enterprise Development LP

Notices

The information contained herein is subject to change without notice. The only warranties for HPE products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the HPE website. HPE has no control over and is not responsible for information outside the HPE website.

Privacy Policy

www.hpe.com/us/en/privacy/master-policy.html

Acknowledgements

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

| | |
|-----------------------------------|-----------|
| Introduction | 4 |
| RDA Enrollment Tool | 5 |
| Connections overview | 5 |
| Connections | 6 |
| Customer-Initiated TLS | 6 |
| HPE-Initiated TLS | 6 |
| HPE-Initiated TLS over IPsec | 7 |
| HPE-Initiated SSH | 7 |
| HPE-Initiated SSH over IPsec | 8 |
| Data and Privacy | 9 |
| Standalone RDA-CAS | 10 |
| Software installation | 10 |
| HPE GPG Signature verification | 10 |
| Virtualization | 11 |
| Secure Shell (SSH) Server | 11 |
| Kernel configuration | 11 |
| Configuration | 11 |
| Configuration data (Outbound) | 12 |
| Configuration data (Inbound) | 13 |
| RDA-CAS Web User Interface (UI) | 14 |
| Access control | 15 |
| OpenSSL library | 15 |
| Enable FIPS mode | 15 |
| Configure backups | 16 |
| Verify installation | 16 |
| Starting the RDA-CAS | 16 |
| Updating the RDA-CAS | 16 |
| Configure automatic updates | 16 |
| Manual update | 17 |
| Uninstall the RDA-CAS | 18 |
| Virtualization | 19 |
| Secure Shell (SSH) Server | 21 |
| Kernel parameters | 22 |
| Supported IPsec parameters | 22 |
| SSL Interception | 23 |

Introduction

HPE Remote Device Access (RDA) is a remote connectivity solution which enables connections to devices on customer networks for remote service delivery, support automation, real time monitoring and quality feedback.

This Install Guide will direct you through the necessary steps to set you up with the connection best suited to your system.

| In this edition you will find: | Typography and Support: |
|--|---|
| <ul style="list-style-type: none"> • Step-by-step RDA Enrollment Tool instructions • RDA-CAS configuration details • Guidelines and infographics • Support options | <p>Green links provide more information or download locations.</p> <p>Notes: provide important information, please read.</p> <p>If you require further support, refer to Get Help from Support and search for your local Response Center.</p> |

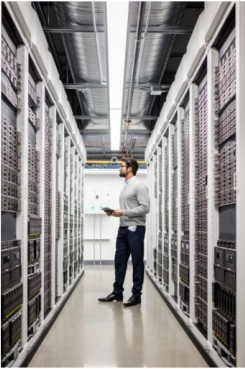
Get started

Determine how you want your device to connect with HPE. Just choose a connection from below that works best for your system: (See ["Connections overview"](#) on the next page for detailed descriptions).

| | |
|--------------------------------|--------------------------------|
| - Customer-Initiated TLS | - HPE-Initiated SSH |
| - HPE-Initiated TLS | - HPE-Initiated SSH over IPsec |
| - HPE-Initiated TLS over IPsec | |

For example, the most popular and best connection, the Customer-Initiated TLS, requires a CAS but does not require enrollment as this will occur automatically. Just simply download the kit, install and configure it.




Proceed to the [Welcome page](#) when ready to start and follow the on-screen instructions provided to:

| | |
|---|---|
|  <p>Remote Device Access</p> <p>Designed for the enterprise, HPE RDA (Remote Device Access) provides integrated remote connectivity for support automation, device telemetry and remote service delivery.</p> <p>Get started</p> <ul style="list-style-type: none"> Enroll or Manage your Device Download RDA Software RDA Documentation Data and Privacy <p>© Copyright Hewlett Packard Enterprise Development LP Terms Privacy Help</p> | <p>Get started:</p> <ul style="list-style-type: none"> • Enroll or Manage your Device Here you start or complete an enrollment. You can also update your connection details. • Download RDA Software This is where you download the specific software you require. • RDA Documentation Open or download the Install Guide or Security Whitepaper. • Data and Privacy You can view or delete your personal information here. See "Data and Privacy" on page 9 for more info. • Get Help from Support For Support, click the link on the Footer. |
|---|---|

RDA Enrollment Tool

You can find the latest RDA Enrollment Tool on the [Welcome page](#).

The inbound tunnel represents a TLS / SSH connection initiated from HPE to the customer CAS system. The connection can be made either directly, over an IPsec tunnel or through SSH. In all cases, HPE requires network connection details to successfully establish the tunnel. The connection details must be provided during a simple 3-step enrollment process to successfully register the CAS system, shown below.

| STEP 1 ...START | STEP 2 ...CONFIGURE | STEP 3 ...COMPLETE |
|---|---|--|
|  |  |  |
| Start an enrollment. Provide HPE connection details, and if required, install / configure the RDA-CAS to your device. | Configure your system. Most setups require configuration at the customer end to allow HPE connections via selected devices. | Complete the enrollment. Provide connection-specific additional details and validate the connection. |
| <p>Overview: Begin with <i>Start an enrollment</i> in the main menu. This will bring you through the steps, followed by the connections list. Select your connection and follow the instructions. HPE recommends you accept connections from all midways to ensure the greatest availability. If you must limit connections select the HPE Midways you will allow to connect to your network. You must accept connections from at least 2 HPE Midways on port 2371 and configure your firewall to accept connections from the selected Midway systems to the same port.</p> <p>Notes:</p> <ul style="list-style-type: none"> - If you do not complete the enrollment within 21 days, you will need to re-enroll the CAS device. - HPE will complete an automated health-check twice per month to validate connectivity. | | |

Connections overview

For HPE RDA, your device can initiate the connection to HPE, or HPE can initiate the connection to you. If the latter, you'll need to configure your firewall, IPsec router or SSH server to accept connections from HPE. The RDA connection type indicates how a tunnel-layer connection is formed between a customer's device and an RDA Midway at HPE. You choose the most appropriate connectivity type.

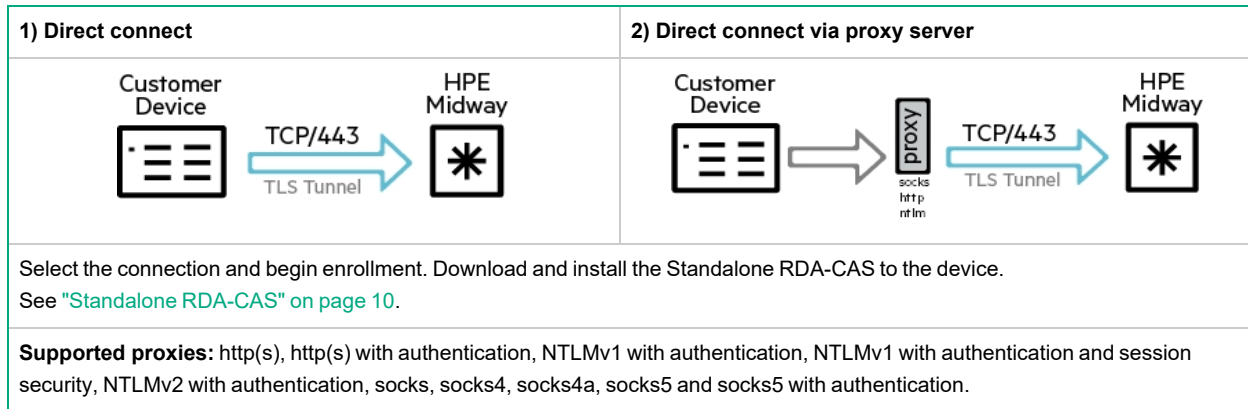
There are two modes for the tunnel. **Outbound** (default) and **Inbound**. Both require NTP (Network Time Protocol) or an equivalent synchronization to the Midway. The **Inbound** tunnel can be established over a direct TLS connection or a pre-configured IPsec connection.

| | |
|-------------------------------------|--|
| Customer-Initiated TLS | The device initiates a connection to HPE, either directly or via a proxy server, over the port TCP / 443. |
| HPE-Initiated TLS | The customer allows HPE to connect to device via TLS 1.2 over the port TCP / 2371. Transiting a NAT firewall is OK. |
| HPE-Initiated TLS over IPsec | HPE will establish an IPsec tunnel to the corporate IPsec router using parameters / credentials that the customer supplies. Through this tunnel, HPE uses a TLS 1.2 transport to provide support. IPsec through NAT is OK. |
| HPE-Initiated SSH | Allow HPE to connect to device via TLS 1.2 over the port TCP / 2371, transiting a NAT firewall is OK. |
| HPE-Initiated SSH over IPsec | HPE will establish an IPsec tunnel to the corporate IPsec router using the parameters / credentials that the user supplies. Through this tunnel, HPE will push an SSH connection to the device. |

Connections

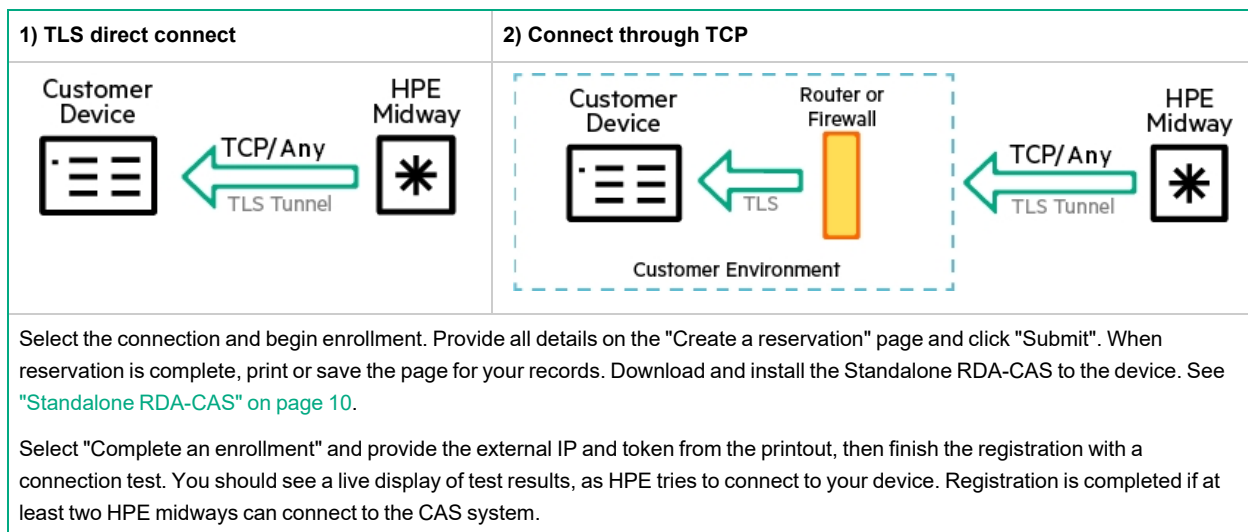
Customer-Initiated TLS

When configured, the device initiates a connection to HPE, either directly or via a proxy server, over the port TCP/443. HPE provides support to you via this connection when required.



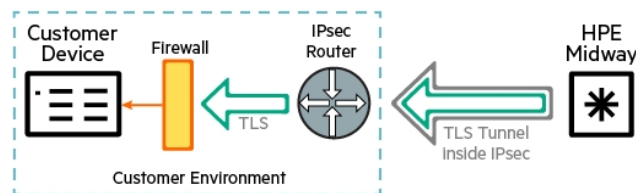
HPE-Initiated TLS

When configured, HPE initiates a connection to your device that will provide support to you. To use this feature, allow HPE to connect to device via TLS 1.2 over the port TCP/2371. Transiting a NAT firewall is OK.



HPE-Initiated TLS over IPsec

When configured, HPE initiates a connection to the device that will provide support to you, the customer. The IPsec tunnel configuration and setup process on the HPE side is now fully automated through the Enrollment tool. To use this feature, HPE will establish an IPsec tunnel to the corporate IPsec router using parameters / credentials that you supply. Through this tunnel HPE will use a TLS 1.2 transport to provide support. IPsec through NAT is OK. HPE recommends to configure your IPsec router to accept connections from all midways to ensure the most availability.



Select the connection and begin enrollment. Provide all details on the "Create a reservation" page and click "Submit". Choose the RDA-CAS subnet with /30 or /32 (single host) subnet mask. The /30 subnet mask will be used by default if not specified otherwise. When reservation is complete, print or save the page for your records. Download and install the Standalone RDA-CAS to the device. See ["Standalone RDA-CAS" on page 10](#).

HPE supports IPsec connection between left and right subnets, where the right subnet (where your CAS system resides in) must have a /30 or /32 subnet mask and the left subnet is a single host subnet with /32 subnet mask.

Enroll multiple CAS devices

It is possible to enroll multiple devices from the same right subnet, when using the /30 subnet mask, where each device uses a different address from that right subnet IP address pool. You will need to enroll each device separately. During this process, make sure to use the same external IP and right subnet at the reservation phase.

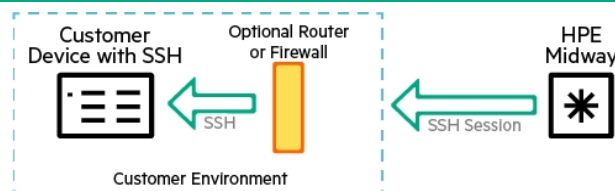
At registration, you will see a list of all IP's from the chosen right subnet. You can choose which CAS / IP you wish to enroll. The enrolled flag helps you identify the CAS devices which have already been enrolled on the given right subnet. You can select an already enrolled IP and this starts a re-enroll of the given CAS device.

Notes:

- HPE supports only the pre-shared key (PSK) IPsec authentication method.
- For supported IPsec parameters please see ["Supported IPsec parameters" on page 22](#).
- The Midway servers do not reside behind a NAT device. The IP provided in the enrollment tool for each Midway represents the real IP address of the given Midway server.

HPE-Initiated SSH

The Standalone RDA-CAS is not required, but an SSH-daemon must run on the device. See ["Secure Shell \(SSH\) Server" on page 21](#) for more info. To provide user support, HPE will initiate a connection to the device using the IP address you supply.

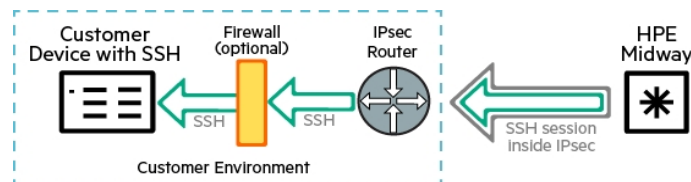


Select connection and begin enrollment. Provide details on "Create a reservation" page and click "Submit".

By default the SSH server runs on port 22. Other ports can be selected: 22, 1022, 2001, 2222, 22222, 50022 or 50023. Selecting a different SSH port during enrollment means that several CAS systems can be behind a single external IP address. When reservation is complete, print / save the page (including public key) for your records.

HPE-Initiated SSH over IPsec

The Standalone RDA-CAS is not required, but an SSH-daemon must run on the device. See ["Secure Shell \(SSH\) Server" on page 21](#) for info. The IPsec tunnel configuration and setup process, on the HPE side, is now fully automated through the Enrollment tool. To provide user support, HPE will establish an IPsec tunnel to the corporate IPsec router using the parameters / credentials that you supply. HPE will then push an SSH connection to the device. Confirm the SSH daemon is running on the port, the internal address is provided and the SSH account for the username exists and is configured as shown in the enrollment.



Select the connection and begin enrollment. Provide all details on the "Create a reservation" page and click "Submit". Choose the RDA-CAS subnet with /30 or /32 (single host) subnet mask. The /30 subnet mask will be used by default if not specified otherwise. When reservation is complete, print or save the page and download or copy the public key for your records.

HPE supports IPsec connections between left and right subnets, where the right subnet (that your SSH server resides in), must have a /30 or /32 subnet mask and the left subnet is a single host subnet with /32 subnet mask.

Enroll multiple SSH servers

It is possible to enroll multiple SSH servers from the same right subnet, when using the /30 subnet mask, where each SSH server uses a different address from that right subnet IP address pool. You will need to enroll each SSH server separately. During the enrollment process, please make sure to use the same external IP and right subnet at the reservation phase.

At registration, you will be presented with a list of all IP's from the chosen right subnet. You can choose which SSH server / IP you wish to enroll. The enrolled flag helps you identify the SSH servers which have already been enrolled on the given right subnet. You can select an already enrolled IP and this will trigger a re-enroll of the given SSH server.

Notes:

- HPE supports only the pre-shared key (PSK) IPsec authentication method.
- For supported IPsec parameters please see ["Supported IPsec parameters" on page 22](#).
- The Midway servers do not reside behind a NAT device. The IP provided in the enrollment tool for each Midway represents the real IP address of the given Midway server.

Additional IPsec info

NAT support

In the case your IPsec router is behind a NAT device, please make sure to provide your IKE local identity at registration. The IKE local identity is sent in the exchange with the remote peer (HPE Midway) to establish communication. HPE will use your external IP as your IKE local identity by default if not specified otherwise. The IKE local identity on most IPsec routers default to the IPv4 address corresponding to the local endpoint, which is different to your external NAT IPv4 address.

IKE version

This is the IKE (Internet Key Exchange) protocol version. Supported IKE versions are IKEv1 and IKEv2. Select the version which matches your IPsec tunnel configuration best. The default is IKEv1.

IKE Local Identity

This is the IKE (Internet Key Exchange) identity of your side of the IPsec tunnel. The local IKE identity is sent in the exchange with the remote peer (HPE Midway) to establish communication. If you do not

configure a local identity on your IPsec router, it uses by default the IPv4 address corresponding to the local endpoint.

The default value for this enrollment setting therefore defaults to the specified external IP.

You can choose to specify your IKE local identity as one of the following: IP address (IPv4), Fully-qualified domain name (FQDN) or an email address.

Note: You need to change the default setting only if your local IKE identity does not equal your external IP. This can be true for example, when you are using Network Address Translation Traversal (NAT-T) where the specified external IP does not match the internal IPv4 address of your IPsec router.

Data and Privacy

In the lower menu section of the [Welcome page](#), there are other options available:

View my personal information

This option securely provides information and what we know about you. It also identifies all the devices associated with your email ID. When an information request is submitted, an encrypted pdf is generated and sent directly back to you in an email. This requires a decryption key to open, which is provided later in the process.

Process

Start the process by clicking the link. Enter your email address in the provided field and click the "Submit" button. On the next page you will receive the encryption key. Use this key to open the pdf, which will be sent to you by email. If you did not receive the email, you may not be associated with any device.

Delete my personal information

This option securely deletes all information associated with your email ID.

Process: Start the process by clicking the link. Enter your email address in the provided field and click the "Submit" button. The email we sent to you contains further instructions and a link to complete the deletion.

Note: Users must complete steps on their device to facilitate the deletion step, see ["Removing contact information" on page 14](#) for more information.

If you fail to complete this step, your contact info is sent to HPE again once the RDA-CAS reconnects to the Midway.

Standalone RDA-CAS

The Standalone RDA-CAS (Remote Device Access-Customer Access Service) is a downloadable software package that provides secure remote access for authorized HPE Support Technicians into your environment.

Software installation

Download the Standalone RDA-CAS package from the [RDA Product Portal](#) UI to your device.

| Action | Command (* = rda-cas version no.) |
|---|---|
| Install the rda-cas package by executing: | CentOS/RHEL: <code>sudo rpm -i rda-cas-*.rpm</code> Debian/Ubuntu: <code>sudo dpkg -i rda-cas-*.deb</code> |


HPE GPG Signature verification

Signing packages with a GNU Privacy Guard (GPG) key allows users to verify the integrity of the received package. Signed with a digital private key that is only held by Hewlett Packard Enterprise Company.

This ensures the package has not been manipulated by a third party.

Note: Only RPM RDA-CAS packages are signed with GPG.

Verification procedure

| 1. Download the keys and fingerprints | |
|--|---|
| These are available to download from the RDA Product Portal . | |
| Click on  Security info and follow instructions on the pop-up. | |
| 2. Import the keys for RPM | |
| Import the public keys while logged in as root by running the following command: | <code>rpm --import downloaded key</code> Example: <code>rpm --import /tmp/rda-rpm-gpg.key</code> |
| 3. Verify using RPM | |
| Use the <code>rpm --checksig</code> command to validate and verify the digital signature of the signed file. The output indicates the validity of the signature: | <code>rpm -checksig <downloaded package></code> Example: <code>rpm --checksig /tmp/rda-cas-1.33-1.e16.x86_64.rpm</code> |

If your file does not pass verification or you do not have the Hewlett Packard Enterprise Company public key installed you will see the following errors:

| Example 1: NOT OK |
|--|
| <pre>rpm --checksig /tmp/rda-cas-1.33-1.e16.x86_64.rpm rda-cas-1.33-1.e16.x86_64.rpm: (SHA1) DSA sha1 md5 (GPG) NOT OK</pre> <p>In this case do not install the rpm. This means the file has been modified in some way since being released from Hewlett Packard Enterprise Company.</p> |

Example 2: MISSING KEY

```
rpm --checksig /tmp/rda-cas-1.33-61.el7.x86_64.signed.rpm
/tmp/rda-cas-1.33-61.el7.x86_64.signed.rpm: RSA sha1 ((MD5) PGP) md5 NOT OK (MISSING KEYS: (MD5) PGP#2497f87c)
In this case the GPG key was not installed. Install the key and run the RPM check again.
```

Skipping the signature check

Skipping is highly discouraged. If your system configuration enforces the signature check but you choose to skip the check, run the `rpm install` command with the '`--nosignature`' flag or `yum` command with '`--nogpgcheck`':

```
rpm -i --nosignature <downloaded package>
Example:
rpm -i --nosignature /tmp/rda-cas-1.33-1.el6.x86_64.rpm
yum localinstall -y --nogpgcheck <downloaded package>
Example:
yum localinstall -y --nogpgcheck /tmp/rda-cas-1.33-1.el6.x86_64.rpm
```

Virtualization

The RDA-CAS is normally installed to a physical Linux OS machine but, if required, can be optionally installed to a VM running any supported OS. Installations and guidelines are found here: ["Virtualization" on page 19](#).

Secure Shell (SSH) Server

The following links provide the information required to get started with Secure Shell. Click on: <https://www.ssh.com/ssh/sshd/> and follow the online instructions.

SSH requires specific configuration for HPE, see ["Secure Shell \(SSH\) Server" on page 21](#) for more details.

Kernel configuration

For optimal kernel performance, see ["Kernel parameters" on page 22](#) for the recommended settings.

Configuration

Once the software is installed, execute the following command to setup and start the RDA-CAS service:

| Action | Command |
|----------------|-----------------------------|
| RDA-CAS setup: | <code>sudo rda-setup</code> |

This will prompt you to enter configuration data to setup and run the RDA-CAS. The RDA-CAS tunnel to the HPE Midway can be established in both directions. Based on the selected direction, the RDA-CAS setup questions will differ. In the case of an Inbound tunnel, you will need to enroll the device and obtain a security token which is required during the setup process, see ["RDA Enrollment Tool" on page 5](#) for more info.

Configuration data (Outbound)

Default data is provided in the square [brackets]. Enter a "?" for a list of options on some of the parameters.

Customer-Initiated TLS connection

| Configuration parameters and description | |
|---|---|
| Tunnel direction (? to list) [outbound] | This indicates the direction: Customer Initiated TLS Connection. |
| WAPI listening IP and port (? to list) [127.0.0.1:8082]: | This is the local IP and port for the RDA-CAS Web UI. |
| Connect Tunnel on Startup [yes]: | Should the tunnel to HPE be started automatically after the RDA-CAS starts. |
| Proxy [none] | Requires the proxy server address the CAS needs to access the HPE Midway. |
| List of features to enable (? to list) [auto-update,ida]: | Can be auto-update and ida (Interactive Device Access). |
| Type new Web-Login password for user 'rda-admin': | This password is set for the rda-admin user and is used for the RDA-CAS Web UI login. |
| Retype new Web-Login password for user 'rda-admin': | Re-type in the new password for user login. |
| Two letter country code or country name: | Submit the customer's two-letter country code or country name. To see the codes list, use: <code>rda-setup --country list</code> . Enter <code>00</code> if your country is not listed. |
| Company name: Company site: | Submit the customer's company name. Submit the customer's company site or location name. |
| Contact name: Contact email: Contact phone number: | Submit the customer's contact name. Submit the customer's contact email. Submit customer's contact phone number. |
| <p>Enter your local contacts, one per line. At least one contact name is mandatory, all others are optional. End the list with an empty name. The first contact is primary. To clear an existing list, enter a single dash for the name.</p> <p>Contacts will be visible in the Support app should there be any issues with the customer's connection with the device.</p> | |
| You must agree to the software license terms to continue. Once agreed you will not be asked again. | |

Configuration data (Inbound)

Default data is provided in the square [brackets]. Enter a "?" for a list of options on some of the parameters.

HPE-Initiated TLS / HPE-Initiated TLS over IPsec connections

| Configuration parameters and description | |
|--|---|
| Tunnel direction (? to list) [inbound]: | This indicates the direction: HPE-Initiated TLS Connection. |
| Receiver listening IP:port (? to list IP's and further port information) []: | Receiver listening IP and port is needed for connection from HPE. User(s). IT Support must ensure that HPE Midways can connect to this IP and port through the user's firewall. Note: The user's firewall must allow incoming connections on port 2371 (RDA IANA registered port) from at least two HPE Midways to this IP and port number. |
| WAPI listening IP:port (? to list IP's) [127.0.0.1:8082]: | This is the local IP and port for the RDA-CAS Web UI. |
| List of features to enable (? to list) [auto-update,ida]: | Can be auto-update and ida (Interactive Device Access). |
| Security token []: | Submit Security token. The token is used to identify the device during registration to the RDA Midway. It is 8 characters divided into 2 and delimited with a hyphen. The security token (valid for 21 days) is generated during the enrollment phase by HPE. |
| Type new Web-Login password for user 'rda-admin': | This password is set for the rda-admin user and is used for the RDA-CAS Web UI login. |
| Retype new Web-Login password for user 'rda-admin': | Re-type in the new password for user login. |
| Two letter country code or country name: | Submit the customers' two-letter country code or country name. To see the codes list, use: <code>sudo rda-setup --country list</code> . Enter <code>00</code> if your country is not listed. |
| Company name: | Submit the customer's company name. |
| Company site: | Submit the customer's company site or location name. |
| Contact name: | Submit the customer's contact name. |
| Contact email: | Submit the customer's contact email. |
| Contact phone number: | Submit customer's contact phone number. |
| <p>Enter your local contacts, one per line. At least one contact name is mandatory, all other are optional. End the list with an empty name. The first contact is primary. To clear an existing list, enter a single dash for the name.</p> <p>Contacts will be visible in the Support app should there be any issues with the customer's connection with device.</p> | |
| You must agree to the software license terms to continue. Once agreed you will not be asked again. | |

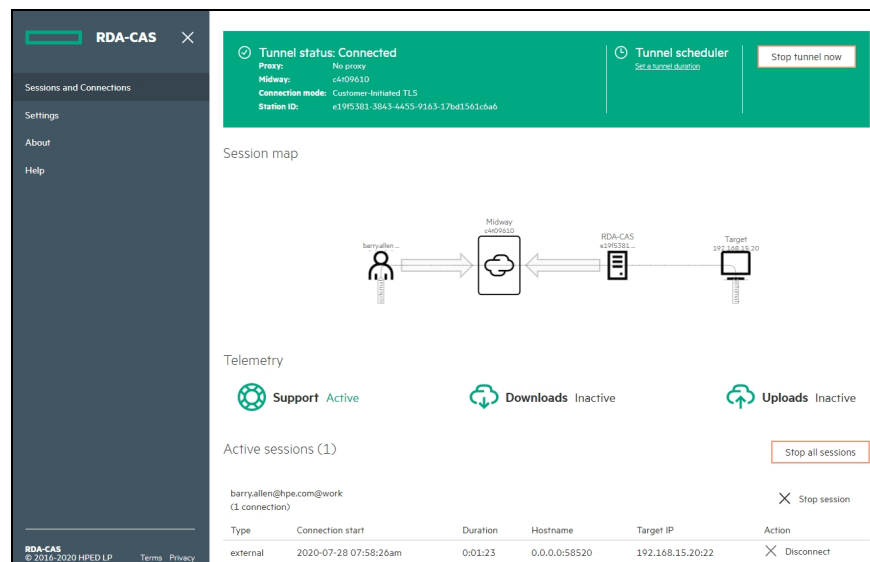
RDA-CAS Web User Interface (UI)

The RDA-CAS provides a management UI which can be accessed at **https://<Web UI IP>:<Web UI port>** (default https://127.0.0.1:8082). In order to login, the user must provide a username (rda-admin) and a strong password (defined during setup).

Notes: Username and password is required only when the listening IP does not equal the loopback address (127.0.0.1). The RDA-CAS management Web UI server uses, by default, a self-signed certificate which is insecure. It is highly recommended to replace this self-signed certificate with a **signed server certificate**, provided by the user, especially if the management UI is accessed from external hosts.

| Action | Command |
|---|---|
| The following steps are required to configure the RDA-CAS management server to use a server certificate provided by the user: | <pre> sudo rda-config -s cas:web-crt-file -v <path_to_certificate> sudo rda-config -s cas:web-key-file -v <path_to_certificate_key> sudo rda-config -s cas:web-ca-file -v <path_to_ca_file> sudo service rda-cas restart </pre> |

The user certificate files must be readable by the user or group the RDA-CAS service is running under (default: rdanet:rdalab). You use the RDA-CAS UI to monitor all active connections, drop connections and verify activity on the RDA-CAS side. Once opened and connected, the RDA-CAS UI will look like this:



Removing contact information

Click the "Settings" tab on the homepage (above) to access user preferences. Then click the "Contacts" tab:

| Designated Contacts + | | | | | |
|---|------------------|--|--------------|--------|--|
| HPE Support Techs can report RDA-CAS issues to a named primary contact. | | | | | |
| Primary | Contact name | Email | Phone | Action | |
| <input checked="" type="radio"/> | Tara J. Brundage | rda_buildbabysitterandtriage_team@groups.ext.hpe.com | 845-555-8157 | | |
| <input type="radio"/> | testasd | asd@asd.com | 98764 | | |

Changes will be visible to the HPE Support Technicians after successful tunnel restart.

Click the "trash" icon to delete details and follow the online instructions.

HPE requires at least one contact remaining. If you cannot provide at least one contact then just uninstall the RDA-CAS.

Access control

Access Control is configurable only through the RDA-CAS Web UI and the default mode is set to **Restricted Access**. Should you require specific user access, you must configure this on the ACL UI. See the RDA-CAS Web UI Online Help for more information.

OpenSSL library

OpenSSL is a robust, commercial-grade, and full-featured toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. It is also a general-purpose cryptography library.

The RDA-CAS package does not provide the cryptographic module (OpenSSL) within the installation package but relies on the host OS to provide one. User can have multiple different OpenSSL library versions installed on the host system. In this case the recommended version will be used (automatically set by rda-setup script on first run).

Supported OpenSSL versions: 1.0.x, 1.1.x., and 3.0.x.

| Action | Command |
|--|--|
| <p>User can define specific OpenSSL library SONAME suffix through configuration parameter in the configuration file (/etc/rda/rda.conf).</p> <p>The SONAME can vary between different operating systems for the same OpenSSL version.</p> <p>Note: Command on the right is an example for OpenSSL version so.1.1.</p> | <pre>sudo rda-config -s dynamic-loader:openssl -v so.1.1</pre> <p>followed by a rda-cas service restart:</p> <pre>sudo service rda-cas restart</pre> |

Enable FIPS mode

The RDA-CAS is FIPS compliant and relies on an open source FIPS 140-2 (Level 1 - OpenSSL 1.x, Level 3 - OpenSSL 3.0.x) validated cryptographic module (OpenSSL).

The Federal Information Processing Standard (FIPS) Publication 140-2, is a computer security standard, developed by a U.S. Government and industry working group to validate the quality of cryptographic modules. The RDA-CAS is FIPS compliant and relies on an open source FIPS 140-2 validated cryptographic module (OpenSSL). Enabling FIPS mode ensures that RDA-CAS uses only FIPS compliant cryptographic algorithms and a FIPS validated cryptographic module (OpenSSL). The RDA-CAS package does not provide the cryptographic module (OpenSSL) within the installation package but relies on the host OS to provide one. In order to enable RDA-CAS in FIPS mode, user must ensure that the host system has installed an OpenSSL version with FIPS module.

| Action | Command |
|--|---|
| <p>RDA-CAS FIPS compliance is enabled by a FIPS-mode configuration parameter in the configuration file (/etc/rda/rda.conf). Users can set the parameter by running following command(s):</p> | <pre>sudo rda-config -s cas:fips -v yes</pre> <p>followed by a rda-cas service restart:</p> <pre>sudo service rda-cas restart</pre> |

If the FIPS mode is enforced on the OS level, RDA-CAS will detect it and switch to FIPS mode regardless of

the configuration parameter value. Please note that RDA backend servers (RDA Midways) are running in FIPS mode by default and that the communication between the RDA-CAS and RDA Midway system is protected by FIPS compliant cryptographic algorithms regardless of the FIPS mode setting on RDA-CAS.

Configure backups

We strongly recommend that you back up the content and subdirectories in the `/etc/rda` directory on a regular basis. This directory contains important configuration information for the RDA-CAS.

Verify installation

| Action | Command |
|--|---|
| To verify the correct version of the RDA-CAS kit is installed, run one of these commands: | CentOS/RHEL: <code>sudo rpm -q rda-cas</code> Debian/Ubuntu: <code>sudo dpkg --get-selections rda-cas</code> |
| To avoid restarting daemons during setup, run the <code>rda-setup</code> command with the <code>--norestart</code> option: | <code>sudo /usr/bin/rda-setup --norestart</code> |
| To view RDA-CAS general config. info, such as the Station ID, execute: | <code>sudo rda-info</code> |

Starting the RDA-CAS

The `rda-setup` script starts the RDA-CAS by default at boot time, as a standard Linux service.

| Action | Command |
|--|--|
| To start the RDA-CAS, execute: | <code>sudo service rda-cas start</code> |
| To stop the RDA-CAS, execute: | <code>sudo service rda-cas stop</code> |
| To disable the automatic service start during bootup, execute: | CentOS/RHEL: <code>sudo chkconfig rda-cas off</code> Debian/Ubuntu: <code>sudo systemctl disable rda-cas</code> |
| To enable a service to be started on bootup, execute: | CentOS/RHEL: <code>sudo chkconfig rda-cas on</code> Debian/Ubuntu: <code>sudo systemctl enable rda-cas</code> |
| To restart the service, execute: | <code>sudo service rda-cas restart</code> |

Updating the RDA-CAS

HPE recommends using the automatic update feature for the RDA-CAS, enabled during `rda-setup`. It will configure the RDA-CAS to check for updates once per day.

Configure automatic updates

You can change the configuration parameters using the RDA configuration tool.

| Action | Command |
|--|--|
| To enable/disable auto-update set the appropriate value: | <code>sudo rda-config -s features:auto-update -v <yes/no></code> |
| Then run <code>rda-setup</code> script: | <code>sudo rda-setup --batch</code> |

Manual update

Since version 1.22 the name of the package has changed from `rda-cas-full` to `rda-cas`.

Depending on which package is currently installed on your system, the update procedure will be different.

Please follow the appropriate manual update procedures, steps described in detail further below.

If you are unsure which package is currently installed on your device, check it with:

| CentOS/RHEL | Debian/Ubuntu |
|--|--|
| <code>sudo rpm -qa grep rda-cas</code> | <code>sudo dpkg -l grep rda-cas</code> |

Updating the rda-cas-full package

Follow this procedure if `rda-cas-full` is installed on your system.

Download the appropriate package for your OS from the [RDA Product Portal](#).

Remove currently installed package with option to leave configuration and temporary files intact enabled:

| CentOS/RHEL | Debian/Ubuntu |
|---|--|
| <code>sudo rpm -e --noscripts rda-cas-full</code> | <code>sudo rm -f</code> <code>/var/lib/dpkg/info/rda-cas-full.postrm</code> <code>sudo dpkg -r rda-cas-full</code> |

Install the new `rda-cas-1.xx` package preserving the old configuration files:

| CentOS/RHEL | Debian/Ubuntu |
|---|---|
| <code>sudo yum localinstall -y --nogpgcheck</code> <code><downloaded package></code> Example: <code>sudo yum localinstall -y --nogpgcheck</code> <code>/tmp/rda-cas-1.22-547.el6.x86_64.rpm</code> | <code>sudo dpkg --force-confold --force-confdef</code> <code>-i <downloaded package></code> Example: <code>sudo dpkg --force-confold --force-confdef</code> <code>-i /tmp/rda-cas_1.22-547+deb8_amd64.deb</code> |
| Note: For CentOS/RHEL, the package manager will not automatically use the previous configuration. You need to move the backups made by the package manager to the correct location (see the next step). | |

Move the backup files (made by the package manager if they exist) to a correct file name:

| CentOS/RHEL | Debian/Ubuntu |
|--|---------------|
| <code>sudo mv -f /etc/rda/rda.conf.rpmsave /etc/rda/rda.conf</code> <code>sudo mv -f /etc/rda/acl-rda.dat.rpmsave /etc/rda/acl-rda.dat</code> <code>sudo mv -f /etc/rda/acl-rest.dat.rpmsave /etc/rda/acl-rest.dat</code> <code>sudo mv -f /etc/pam.d/rda-cas.rpmsave /etc/pam.d/rda-cas</code> | n/a |
| Note: For CentOS/RHEL, in case a specific file doesn't exist, just skip it. | |

Run the setup script in silent mode to finish. Also for Debian/Ubuntu, you must purge any remaining parts:

| CentOS/RHEL | Debian/Ubuntu |
|---|---|
| <code>sudo rda-setup --batch</code> | <code>sudo rda-setup --batch</code> <code>sudo dpkg -P rda-cas-full</code> |
| Note: The settings will be picked up from previous configuration file. | |

Updating the rda-cas package

Follow this procedure if `rda-cas` is installed on your system.

Check the [RDA Product Portal](#) for a new version of the RDA-CAS for your operating system.

| Action | Command |
|--|---|
| To manually check for updates, execute as root: (If an update is available the latest version of the RDA-CAS is returned). | CentOS/RHEL: <code>sudo yum clean all</code> <code>sudo yum check-update rda-cas</code> Debian/Ubuntu: <code>sudo apt-get clean</code> <code>sudo apt-get update</code> |
| To install the latest version of the RDA-CAS, execute: | CentOS/RHEL: <code>sudo yum install rda-cas -nogpgcheck</code> <code>sudo rda-setup</code> Debian/Ubuntu: <code>sudo apt-get --only-upgrade install rda-cas</code> <code>sudo rda-setup</code> |
| Note: The RDA-CAS CA (Certificate Authority) bundle <code>rda-ca.pem</code> is maintained by HPE. | |

Uninstall the RDA-CAS

This command removes the whole RDA-CAS package and all its configuration files from the device.

| Action | Command |
|--|---|
| Determine the installed package name: | CentOS/RHEL: <code>sudo rpm -qa grep rda-cas</code> Debian/Ubuntu: <code>sudo dpkg -l grep rda-cas</code> |
| To uninstall <code>rda-cas</code> , execute: | CentOS/RHEL: <code>sudo rpm -e <rda-cas/rda-cas-full></code> Debian/Ubuntu: <code>sudo dpkg -P <rda-cas/rda-cas-full></code> |

Virtualization

About VirtualBox/VMware ESXi

The Oracle VM Virtualbox is a cross-platform virtualization application that must be installed to your Operating System, before installing and running the RDA-CAS. See <https://www.virtualbox.org/> for more info.

The VMware ESXi is an enterprise-class, type-1 Hypervisor (or Virtual Machine Monitor) software, firmware or hardware that creates and runs virtual machines. It includes and integrates vital OS components such as a kernel. See <https://my.vmware.com/en/web/vmware> for more info.

VM prerequisites

To run VirtualBox and VMware ESXi

Check Virtualization sites for exact parameters. You will need a working **Internet** connection and reasonably powerful host hardware. Ensure you have enough disk space and RAM for VM installation and usage on the host system. **Note:** Before guest OS is installed, check if the virtualization parameters in the **BIOS** is **enabled**.

VM installation

| VirtualBox | ESX/ESXi |
|--|--|
| Download the latest version of the virtualization software from: https://www.virtualbox.org/ and follow the online instructions. | Download latest version of the virtualization software from: https://my.vmware.com/en/web/vmware/ and follow the online instructions. |

VM Guest OS installation

Recommended requirements

You will need a working Internet connection, hard disk space of **10 GB** for installation (mostly for the guest OS) and **1** dedicated processing core. At least **1 GB RAM** for the Guest OS. See the Product Portal for supported guest operation systems.

| VirtualBox | ESX/ESXi |
|---|---|
| <ul style="list-style-type: none"> Download supported Linux OS image onto the host where VirtualBox is installed. Create new machine within the VirtualBox manager. Set basic machine parameters, e.g. the machine name, ram/disk size, etc. Point storage IDE controller CD/DVD to the downloaded Linux OS image file. Leave network settings to default NAT, install OS. | <ul style="list-style-type: none"> Download supported Linux OS image onto the host where ESX/ESXi is installed. Create new virtual machine from the vSphere Client. Go through the steps of creating a new VM. Select appropriate Guest system template, (so wizard can load some defaults to the system), and set the network card and the device's hard drive. Connect Linux ISO file to the VM's IDE controller. |
| Note: In order to benefit opening RDA-CAS web UI via a desktop or menu shortcut, a desktop environment must be selected during the install (GNOME, KDE, ...). SSH server is also recommended. | |

Prep for guest VM installation

| VirtualBox | ESXi |
|---|---|
| <ul style="list-style-type: none"> • Configure your network settings on the new system for RDA-CAS to reach the internet. • If required in user network, include correct proxy configuration. Include OS package managers (apt on Debian/Ubuntu, rpm and yum on CentOS/RHEL). • Package dependencies for the RDA-CAS (if required) must be resolved prior to installing it. • If the system is missing some of the packages then they must be installed separately. Check Support notes for more information. | <p>Access to a VMware VSphere Server and confirm that VMware vSphere Client is installed.</p> <p>If you require to connect through proxy, the following system package manager settings have to be set before you start installing the RDA-CAS:</p> <ul style="list-style-type: none"> • If using Debian/Ubuntu based system: apt-get, dpkg – on both proxy has to be applied. • If using CentOS/RHEL based system: yum and rpm have to have the proxy set. |

Dependencies

| Install dependency commands | |
|--|--|
| CentOS/RHEL: <code>sudo yum install<dependency></code> e.g.: <code>sudo yum install perl-URI</code> | Debian/Ubuntu: <code>sudo apt-get install<dependency></code> e.g.: <code>sudo apt-get install apt-transport-https</code> |
| <ul style="list-style-type: none"> - perl (minimal version 5.0) - perl-URI - dmidecode - openssl - bind-utils - initscripts - net-tools | <ul style="list-style-type: none"> - perl - liburi-perl - dmidecode - openssl - libcurl3 - net-tools |

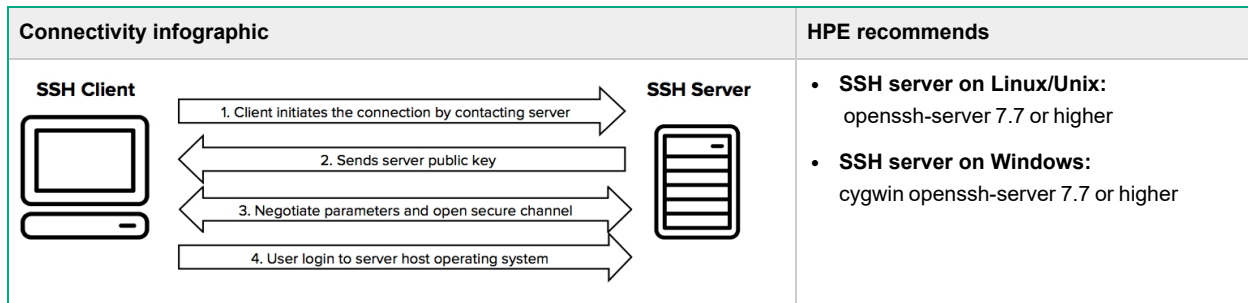
Support notes

If you need additional support, refer to [Get Help from Support](#) and search for your local Response Center.

| VirtualBox/ESXi |
|---|
| <p>While installing the RDA-CAS package, e.g. on CentOS/RHEL, you get an error: Failed dependencies</p> <p>perl-URI is needed by RDA-CAS</p> |

Secure Shell (SSH) Server

Secure Shell (SSH) is a cryptographic network protocol used to provide secure connectivity over an unsecure network, best used in a client-server architecture, connecting remote support to client servers. See <https://www.ssh.com/> for more information.



Prerequisites

| Download and installation instructions |
|--|
| <p>Download the latest version of the SSH Server software from: https://www.ssh.com/ssh/#sec-Download-client-software and follow the online instructions.</p> <p>Check SSH sites for exact parameters. You will need a working Internet connection and reasonably powerful hardware. Ensure you have enough disk space and RAM for installation and usage on the system.</p> |

SSH configuration

For HPE-Initiated SSH connections, we will require an SSH running on your customer site. The HPE RDA Midways will drive connections to this externally accessible server on port 22.

| | |
|------------------------|--|
| Authentication | <p>There are two options on how to configure your SSH, you can use a public/private key pair or password to authenticate the HPE Midway system.</p> <p>Public key: When you reserve you will be given a public key. This must be stored in authorized keys (typically located in the home directory of the user account) on the SSH.</p> <p>Password: When you reserve you will be required to enter the password of the SSH. The SSH must have password authentication enabled (this is disabled by default on most SSH servers).</p> <p>HPE strongly recommends that you use the public/private key pair authentication mode because it is the solution providing enhanced security.</p> |
| Session account | <p>For both authentication methods, the credentials need to be associated with an SSH session account username, which needs to be provided while enrolling the system. For RDA to connect to the SSH server, the account does not need to support full remote shell capabilities. It is sufficient to only allow the SSH session connection. HPE recommends to use a dedicated account only used for RDA connections.</p> |
| Firewall | <p>You will have to open up your firewall so the IP address of that SSH server is accessible from the HPE RDA Midways on port 22.</p> |
| Fingerprint | <p>Once the SSH is successfully enrolled, its server's host key fingerprint is returned and displayed on the UI. Please make sure it matches the key on the customer server itself. The fingerprint is stored on the backend and for every connection attempt compared with the current RSA key, this is to ensure that the Midways always connect to the same system. If the server key changes on the customer system, the device needs to be re-enrolled.</p> |

Kernel parameters

Recommended kernel parameters

```
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_sack = 1
net.ipv4.tcp_timestamps = 1
net.core.rmem_max should be a minimum of 12582912
net.core.wmem_max should be a minimum of 12582912
net.ipv4.tcp_mem = "364992 486656 729984"
net.ipv4.tcp_rmem = "10240 87380 12582912"
net.ipv4.tcp_wmem = "10240 87380 12582912"
```

Note: If user does not use the recommended parameters, the following warning will occur:
WARN: \$key is set to \$current_value. For optimal RDA performance, we recommend: \$wanted_value.

| | |
|------------------------|--|
| \$key | This is the name on the left, i.e. "net.ipv4.tcp_window_scaling". |
| \$current_value | This is the kernel parameter value that is set at that moment on the CAS. |
| \$wanted | This is the value that we want, i.e. the values on the right, see above table. |

Supported IPsec parameters

| IKE parameters | |
|--------------------------------|---|
| Version | IKEv1 / IKEv2 |
| Authentication method | Preshared keys only |
| Crypto | AES / AES-192 / AES-256 |
| Data integrity | SHA1 / SHA2-256 / SHA2-384 / SHA2-512 |
| Diffie-Hellman group (phase 1) | Group 5 / 14 / 15 / 16 / 17 / 18 / 22 / 23 / 24 |
| Timer IKE phase 1 | 28800 |
| Timer IKE phase 2 | 14400 |
| Type | Main mode |

| IPsec parameters | |
|-------------------------------|--|
| UDP encapsulation | Yes, customer NAT is supported |
| Protocol | ESP |
| Crypto | AES / AES-192 / AES-256 / AES-GCM128 / AES-GCM192 / AES-GCM256 |
| Data integrity | SHA1 / SHA2-256 / SHA2-384 / SHA2-512 |
| Diffie-Hellman group | Group 5 / 14 / 15 / 16 / 17 / 18 / 22 / 23 / 24 |
| Perfect Forward Secrecy (PFS) | Enabled |

SSL Interception

Server certificate update

(/etc/rda/rda-ca.pem update; only CAS version >1.8 already has an ok certificate).

We have seen two types of customer proxies completing a SSL Interception. They are called "Bluecoat" and "Zscaler". The proxy acts like a "man-in-the-middle" attack performing the SSL Intercept.

You will see an error like this:

```
Mar 18 03:42:05 SP0001648344 rda-cas: WRN [relay.cpp:2113] Could not start tunnel to
tcp:15.241.136.80:443: transport connect: SSL error: Connect fail; protocol error; certificate verify
failed; We do not recognize the identity of midway(s) you are connecting to; either these are impostor
midway systems, or your RDA certificate authority list is out of date. Contact HPE RDA Support to obtain
an updated /etc/rda/private/rda-ca.pem file.
```

To verify it uses curl:

```
curl --insecure -v -x http://user:password@<proxy-host>:<proxy-port>
https://g9t6659g.houston.hpe.com/self
```

If the proxy is performing an SSL Intercept then you will see the following:

Server certificate:

| | |
|----------|--|
| Subject: | CN=g9t6659g.houston.hpe.com,O=Hewlett Packard Enterprise Company,L=Palo Alto, ST=California,C=US |
| Issuer: | CN=lrcicf01.isd.lacounty.gov,L=Downey, ST=California, C=US |

It should only read like this:

Server certificate:

| | |
|----------|--|
| Subject: | CN=g9t6659g.houston.hpe.com,O=Hewlett Packard Enterprise Company,L=Palo Alto, ST=California,C=US |
| Issuer: | CN=DigiCert Global CA G2,O=DigiCert Inc,C=US |

The simple solution is to:

Work with the customer to add RDA midways to a whitelist so that SSL interception does not happen.

Note: Customers may have to disable protocol inspection.

Open Source Licenses

OpenSSL License

Copyright © 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistribution of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright © 1995-1998 Eric Young (ey@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program start up or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistribution of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes cryptographic software written by Eric Young (ey@cryptsoft.com)" The word 'cryptographic' can be left out if the routines, from the library being used, are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgment: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION). HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Raphael License

Copyright © 2008 Dmitry Baranovskiy

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sub-license, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ENVIRONMENTALISM. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

jQuery License

Copyright © jQuery Foundation and other contributors,
<https://jquery.org/>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sub-license, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Grommet License

Apache License Version 2.0, January 2004
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION,
AND DISTRIBUTION.

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution".

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sub-license, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Linux-PAM License

Unless otherwise *explicitly* stated the following text describes the licensed conditions under which the contents of this Linux-PAM release may be distributed:

Redistribution and use in source and binary forms of Linux-PAM, with or without modification, are permitted provided that the following conditions are met:

1. Redistribution of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistribution in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

Alternatively, this product may be distributed under the terms of the GNU General Public License, in which case the provisions of the GNU GPL are required instead of the above restrictions. (This clause is necessary due to a potential conflict between the GNU GPL and the restrictions contained in a BSD-style copyright).

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

curl License

Copyright © 1996 - 2016, Daniel Stenberg, daniel@haxx.se, and many contributors, see the THANKS file. All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

zlib License

zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.8, April 28th 2013.

Copyright © 1995-2013 Jean-loup Gailly and Mark Adler.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler jloup@gzip.org
madler@alumni.caltech.edu