Pulse Secure, LLC
2700 Zanker Road, Suite 200 San Jose, CA 95134

The Pulse Secure Logo, the Pulse logo, and PulseE are trademarks of Pulse Secure, LLC. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

Products made or sold by Pulse Secure or components thereof might be covered by one or more of the following patents that are owned by or licensed to Pulse Secure: 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.

Software Defined Perimeter Deployment Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://www.pulsesecure.net/support/EULA. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.
Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1R1, 1.2</td>
<td>July 2019</td>
<td>Updated the “Adding a Device Certificate to a AAA Service for SDP” section.</td>
</tr>
<tr>
<td>9.1R1, 1.1</td>
<td>June 2019</td>
<td>Updated the “Prerequisites for SDP” section to include Pulse Workspace activation.</td>
</tr>
<tr>
<td>9.1R1, 1.0.1</td>
<td>May 2019</td>
<td>Cosmetic changes</td>
</tr>
<tr>
<td>9.1R1, 1.0</td>
<td>May 2019</td>
<td>Initial publication</td>
</tr>
</tbody>
</table>
# Table of Contents

Revision History ......................................................................................................................... 3
Introduction .................................................................................................................................... 5
  General Note .............................................................................................................................. 5
Overview of SDP ............................................................................................................................ 6
  Network Architecture ................................................................................................................ 7
Prerequisites for SDP .................................................................................................................... 8
  Configuring AWS for SDP .......................................................................................................... 8
Creating an SDP Controller ......................................................................................................... 17
  Creating an SDP Controller on vSphere .................................................................................. 17
  Configuring a AAA Service for SDP ...................................................................................... 24
Creating an SDP Gateway ........................................................................................................... 34
  Configuring an SDP Gateway on vSphere ........................................................................... 34
  Creating an SDP Gateway on AWS ....................................................................................... 35
  Adding an Existing PCS Appliance ........................................................................................ 48
Managing Application Access on a AAA Service ....................................................................... 52
  Creating a Resource Profile on a AAA Service ................................................................... 52
  Adding an Application to an SDP Gateway ......................................................................... 52
  REST API Commands ............................................................................................................ 53
Accessing the End User Portal on Pulse One ............................................................................. 58
SDP Enabled Pulse Desktop Client ............................................................................................. 59
SDP Enabled Pulse Desktop Client Onboarding .......................................................................... 61
  Scenario 1 – User based Onboarding .................................................................................. 61
  Scenario 2 – Browser based Onboarding ............................................................................ 68
Multiple Tunnels Support for SDP Enabled Pulse Desktop Client ............................................ 71
  Configuring L3 Split Tunnel for an SDP Gateway ............................................................... 72
  Configuring PSAM Tunnel for an SDP Gateway ................................................................. 73
SDP Enabled Pulse Desktop Client Configuration Settings ...................................................... 77
Troubleshooting .......................................................................................................................... 83
Requesting Technical Support ................................................................................................... 86
  Self-Help Online Tools and Resources ............................................................................... 86
  Opening a Case with PSGSC .................................................................................................. 86
References ................................................................................................................................... 87
Introduction

This document describes the process of configuring a Software Defined Perimeter system.

- Overview of SDP
- Prerequisites for SDP
- Creating an SDP Controller
- Creating an SDP Gateway
- Managing Application Access on a AAA Service
- Accessing the End User Portal on Pulse One

Once you have an SDP controller and all required SDP gateways, you can configure your SDP appliances to perform their required SDP role.

General Note

- Avoid resource policies that give everyone access to everything.
  - In each PCS and in the SDP AAA service, go to Users > Resource Policies > VPN Tunneling > Access control. If the Initial VPN Tunneling Policy is present and if it allows All roles access to *:*; remove the policy. Add more-specific policies instead.
  - In each PCS and in the SDP AAA service, go to Users > Resource Policies > Web > Web ACL. If the Initial Policy for Local Resources is present, remove it. Add more-specific policies instead.
  - Rather than manually making these changes on every PCS, you can put all of the PCS appliances into a Pulse One configuration group. You can make the change on the master appliance of the group and publish the change to all of the other members. This option is not available for SDP gateways, however.
- Be careful about virtual desktops. Depending on your network's design, a virtual desktop may have access to your entire network. Even if resource policies prevent a user from directly accessing a particular resource/application, their virtual desktop might still be able to access the resource/application. Consider using a firewall or similar technology to prevent this.
- All of this advice pertains to all PCS appliances in your enterprise – whether they are SDP gateways or not. A PCS that is not an SDP gateway can still allow bypassing SDP policies.
Overview of SDP

Traditional network-based security (Network Defined Perimeter) architectures use firewalls on the network perimeter to limit access to public IP addresses. This exposes the network to a variety of network-based attacks.

Connectivity in a Software Defined Perimeter system is based on a need-to-know model, in which mobile devices are verified and authorized before access to application infrastructure is granted. Application infrastructure cannot be detected remotely, and has no visible DNS information or exposed IP addresses. This protects networked resources from many common network-based attacks.

Pulse Secure SDP uses AAA service which individually act as either an SDP controller or an SDP gateway. Mobile users perform authentication on an SDP controller which runs an Authentication, Authorization and Accounting (AAA) Service. The SDP controller then enables direct communication between the user and the SDP gateways that protect the user’s authorized resources, and enables requested encryption. This does not require the general exposure of public IP addresses. It also separates the control plane and the data plane.

Pulse Secure SDP supports a number of network topologies, and can include both cloud-based and data center-based resources.

**Figure 1: Software Defined Perimeter – Network Topology**

![Software Defined Perimeter – Network Topology](image)
Network Architecture

In this reference architecture, Gateways and the Controllers reside in the DMZ network at the entry point of the Internet ingress, with edge firewalls controlling access to the gateways.
Prerequisites for SDP

You must perform the following tasks before creating your SDP network:

- Ensure that you have added a license that supports SDP to your Pulse One. The license number will have the general form P1-SDP-xxxxxxx-xxxxxxx. Also, ensure you have activated Pulse Workspace using the Try Pulse Workspace option. See the Pulse Software Defined Perimeter Getting Started Guide for full details of this process.
- In Pulse One, ensure the following are set under Workspace Properties:
  - “SDP Provision Certificate” is set to Yes.
  - “Use Windows CA server CAWE to request SDP device certificates” under “Enterprise PKI Integration” is set to Yes. For details about the configuration of Enterprise PKI server, refer to Pulse Workspace Administration Guide.
- (vSphere only) Ensure that your vSphere host is synched to an NTP server. Failure to do this may result in certificate verification issues that cause auto-registration of any resulting AAA service to fail. Refer to the VMware vSphere documentation for details of this operation.
- (AWS only) Ensure that you have AWS credentials based on IAM authorization.

  Note: You cannot create an SDP gateway on AWS using standard AWS credentials.

- (AWS only) Ensure that AWS is configured correctly to use SDP, see Configuring AWS for SDP.

Configuring AWS for SDP

This section describes how to configure AWS to prepare for SDP.

To configure AWS for SDP, you must:

- Ensure that you are using AWS credentials that are based on IAM authorization.

  Note: You cannot create an SDP gateway on AWS using standard AWS credentials.

- Create an IAM policy to support SDP, see Creating an IAM Policy to Support SDP.
- Assign the IAM policy to the user/group who will create the SDP gateways:
  - Assigning an IAM Policy to a User
  - Assigning an IAM Policy to a Group

Creating an IAM Policy to Support SDP

You must create and configure an IAM policy called PulseOneSDPOrchestrationPolicy to enable the creation of an SDP gateway on AWS.

To create the required IAM policy:

1. Log into the AWS Management Console as an administrator.
2. On the AWS top bar, click Services and then locate the Security, Identity, & Compliance options.

   The IAM Dashboard appears.

   ![Figure 2: AWS IAM Dashboard](image)

4. On the left menu, select **Policies**.

   The IAM Policies page appears.

   ![Figure 3: AWS IAM Policies](image)

5. Click **Create policy**.

   The IAM Create policy page appears.

   ![Figure 4: AWS IAM Create Policy](image)

6. Select the **JSON** tab.
7. In the JSON tab, delete the default text and paste in the following JSON definition in its entirety:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupIngress",
                "route53:GetChange",
                "ec2:DeleteTags",
                "route53:GetHostedZone",
                "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
                "ec2:DeleteVolume",
                "ec2:StartInstances",
                "ec2:RevokeSecurityGroupEgress",
                "route53:ListResourceRecordSets",
                "iam:ListAttachedUserPolicies",
                "iam:ListAttachedGroupPolicies",
                "ec2:DetachVolume",
                "ec2:RebootInstances",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
                "ec2:TerminateInstances",
                "ec2:CreateTags",
                "iam:ListGroupPolicies",
                "route53:ChangeResourceRecordSets",
                "ec2:RunInstances",
                "iam:ListUserPolicies",
                "ec2:StopInstances",
                "iam:ListInstanceProfiles",
                "ec2:CreateVolume",
                "ec2:RevokeSecurityGroupIngress",
                "iam:ListGroupsForUser",
                "ec2:DeleteSecurityGroup",
                "iam:GetUser"
            ],
            "Resource": [
                "arn:aws:route53:::hostedzone/**",
                "arn:aws:route53:::change/**",
                "arn:aws:ec2::*:subnet/*",
                "arn:aws:ec2::*:key-pair/*",
                "arn:aws:ec2::*:instance/*",
                "arn:aws:ec2::*:volume/*",
                "arn:aws:ec2::*:security-group/**",
                "arn:aws:ec2::*:network-interface/**",
                "arn:aws:ec2::*:image/**",
                "arn:aws:iam::*:instance-profile/**",
                "arn:aws:iam::*:user/**",
                "arn:aws:iam::*:group/**
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "ec2:DisassociateAddress",
                "ec2:DescribeAddresses",
                "ec2:DescribeInstances",
                "ec2:UnmonitorInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRegions",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAvailabilityZones",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeVolumes",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeRouteTables"
            ]
        }
    ]
}
```
"ec2:DescribeInstanceStatus",
"ec2:ReleaseAddress",
"ec2:DetachNetworkInterface",
"ec2:DescribeTags",
"ec2:ModifyNetworkInterfaceAttribute",
"route53:ListHostedZones",
"ec2:DeleteNetworkInterface",
"ec2:AssignPrivateIpAddresses",
"ec2:AllocateAddress",
"ec2:DescribeInstanceCreditSpecifications",
"ec2:DescribeSecurityGroups",
"ec2:CreateNetworkInterface",
"ec2:DescribeImages",
"ec2:DescribeVpcs",
"ec2:AttachNetworkInterface",
"ec2:AssociateAddress",
"ec2:DescribeSubnets"
],
"Resource": "*
}
}

8. Under the text box, click **Review policy**.

**Figure 5: AWS IAM Create Policy Text**

The **Review policy** page appears.

9. Enter the **Name** as “PulseOneSDPOrchestrationPolicy” exactly.

**Figure 6: AWS IAM Review Policy**
10. Click **Create policy**.

A confirmation message appears on the Policies page.

**Figure 7: AWS IAM Policy Created**

![PulseOneSDPOrchestrationPolicy has been created.](image)

The policy is complete. The next process is to assign the policy to the IAM user who will create the SDP appliances, see [Assigning an IAM Policy to a User](#).

**Assigning an IAM Policy to a User**

After you have created the required IAM policy to support SDP, you can assign the policy to the IAM user who will implement SDP.

> **Note:** Alternatively, you can assign the policy to the group whose users will implement SDP, see [Assigning an IAM Policy to a Group](#).

To assign an IAM policy to a user:

1. Log into the AWS Management Console as an administrator.
2. On the AWS top bar, click **Services** and then locate the **Security, Identity, & Compliance** options.
   
The IAM Dashboard appears.
4. On the left menu, select **Users**.
   
The IAM Users page appears.
5. Locate and select the required IAM admin user.
   
The user profile Summary appears.

**Figure 8: AWS IAM User Profile Summary**

![AWS IAM User Profile Summary](image)
6. Click **Add permissions**.

   The Add permissions page appears.

   **Figure 9: AWS IAM User Add Permissions**

   ![Add permissions page](image.png)

7. Select **Attach existing policies directly**.

8. Select the check box for *PulseOneSDPOrchestrationPolicy*.

9. Click **Review**.

   A summary page appears.

   **Figure 10: AWS IAM User Add Permissions Summary**

   ![Summary page](image.png)
10. Review the displayed information and click **Add permissions**.

    The policy is added to the user profile **Summary**.

    **Figure 11: AWS IAM Updated User Profile Summary**

Once this process is complete, IAM is fully configured for SDP.

**Assigning an IAM Policy to a Group**

After you have created the required IAM policy to support SDP, you can assign the policy to the group whose users will implement SDP.

- **Note:** Alternatively, you can assign the policy directly to a user who will implement SDP, see **Assigning an IAM Policy to a User**.

1. Log into the AWS Management Console as an administrator.
2. On the AWS top bar, click **Services** and then locate the **Security, Identity, & Compliance** options.

    The IAM Dashboard appears.
4. On the left menu, select **Groups**.

    The IAM Groups page appears.
5. Locate and select the required IAM group.
   The group Summary appears.

   **Figure 12: AWS IAM Group Profile Summary**

   ![AWS IAM Group Profile Summary](image)

6. Click **Attach policy**.
   The Attach Policy page appears.

   **Figure 13: AWS IAM User Add Permissions**

   ![AWS IAM User Add Permissions](image)

7. (Optional) Use the **Filter** options to locate the *PulseOneSDPOrchestrationPolicy* policy.

8. Select the check box for *PulseOneSDPOrchestrationPolicy*. 
9. Click **Attach Policy**.

   The policy is added to the group profile Summary.

**Figure 14: AWS IAM Updated Group Profile Summary**

![AWS IAM Updated Group Profile Summary](image)

Once this process is complete, IAM is fully configured for SDP.
Creating an SDP Controller

After you have performed any prerequisite tasks (see Prerequisites for SDP), you can create a single SDP controller as a virtual AAA service on vSphere.

Notes:
- You cannot create an SDP controller on the AWS platform. But you can add one that is already existing on the AWS platform.
- You cannot create more than one controller on Pulse One.

To do this, perform the following steps:
- Creating an SDP Controller on vSphere
- Configuring a AAA Service for SDP

Creating an SDP Controller on vSphere

You can create a single SDP controller as a virtual AAA service on vSphere.

This process creates the VM appliance and performs all required registration activities on the appliance automatically.

Note: This process requires sufficient appliance licensing capacity on Pulse One.

Note: Before beginning this process, ensure that your vSphere host is synched to an NTP server. Failure to do this may result in certificate verification issues that cause auto-registration of any resulting AAA service to fail. Refer to the VMware vSphere documentation for details of this operation.

Note: During this process, you can optionally use a master appliance template. A master template encapsulates an existing deployed appliance, and enables the re-use of many configuration settings on any appliance that is deployed using the template. To create a master template, see the Pulse Secure Pulse One documentation.

To create and register a AAA service as a VM on vSphere:
1. Start Pulse One.
2. Click the Appliances menu and then the Appliances tab.
   The Appliances tab displays all current appliances.
3. Click **Add Appliance**.

The Add Appliance wizard starts.

**Figure 15: Add Appliance**

4. Select **Create virtual appliance in VMware vSphere** and click **Next**.

The vSphere Credentials panel of the wizard appears.

**Figure 16: vSphere Credentials**

5. Complete the properties for this panel of the wizard.

For the first use of this wizard:

   - For **Account**, select **Add New**.
   - For **Hostname**, enter the FQDN or IP address of your vCenter host.

   **Note:** The use of a standalone ESX host is not supported for SDP.

   - For **Username** and **Password**, enter your vSphere credentials.

For later uses of the wizard, select the required **Account**. The credentials for this are stored, and do not need to be entered.
6. Click **Next**.

The Appliance Configuration panel of the wizard appears.

**Figure 17: Appliance Configuration**

![Appliance Configuration Panel]

7. Enter the **Appliance Name**. This will be the displayed name in the list of appliances and will also be used to automatically populate the **Internal FQDN** and **External FQDN** properties on subsequent wizard panels.

8. If you are creating a AAA service for use with SDP, select the required **SDP Mode** (either **Disabled** or **AAA service**).

   By default, **SDP Mode** is set to **Disabled**. This is correct for all non-SDP appliances.

9. Specify additional information for the appliance:
   - A **Company Name**.
   - The **Appliance Username, Password** (and **Confirm Password**) for a required user on the appliance. This user will be created once the appliance is created.
   - Note that the **SDP License Auth Code** field currently does not use the licenses added here.

10. Click **Next**.

The Appliance Network Configuration panel of the wizard appears.

**Figure 18: Appliance Network Configuration: DNS Settings**

![DNS Settings Panel]
11. Specify the **Primary DNS** and the **Secondary DNS** for your network.

**Note:** The displayed values are examples, and not defaults.

12. Expand the **Internal Network Settings** panel.

**Figure 19: Appliance Network Configuration: Internal Network Settings**

13. In the **Internal Network Settings**:

- For **Private Domain Name**, enter the internal domain name for your appliance.

  **Note:** When you shift focus away from this property, the **Private Domain Name** setting is displayed as a suffix to **Internal FQDN**.

- The **Internal FQDN** property is populated automatically using the **Appliance Name** you specified in the **Appliance Configuration** wizard panel, with the **Private Domain Name** used as a suffix. Change the Internal FQDN as required.

- For **Internal Network Port Group**, enter a name for the vSphere network. For example, **VM Network**.

- For **IP Address**, enter the required internal IP address of the appliance.

- For **Subnet** and **Gateway**, enter the required subnet mask and gateway IP address.

- (Optional) For **Default VLAN ID**, enter your numeric VLAN identifier.
14. Expand the **External Network Settings** panel.

![Figure 20: Appliance Network Configuration: External Network Settings](image)

15. In the **External Network Settings**:

   - **Public Domain Name** automatically uses the FQDN of your Pulse One appliance. This field is auto-populated and is read-only.

     ▪ Note: When you shift focus away from this property, the **Public Domain Name** setting is displayed as a suffix to **External FQDN**.

   - **External FQDN** automatically prefixes the Public domain name with `aaa` i.e. aaa.<p1-FQDN>.. This field is auto-populated and is read-only.

   - For **External Network Port Group**, enter a name for the vSphere network. For example, **VM Network**.

   - For **IP Address**, enter the required external IP address of the appliance.

   - For **Subnet** and **Gateway**, enter the required subnet mask and gateway IP address.

   - (Optional) For **Default VLAN ID**, enter your numeric VLAN identifier.
16. Expand the Management Network Settings panel.

**Figure 21: Appliance Network Configuration: Management Network Settings**

![Management Network Settings Panel](image)

17. In the Management Network Settings:

- For Management Domain Name, enter a name for the vSphere network. For example, VM Network.
- For Management Network Port Group, enter a name for the vSphere network. For example, VM Network.
- For IP Address, enter the required management IP address of the appliance.
- For Subnet and Gateway, enter the required subnet mask and gateway IP address.
- (Optional) For Default VLAN ID, enter your numeric VLAN identifier.

18. Click Next.

The vSphere Configuration wizard panel appears.

**Figure 22: vSphere Configuration**

![vSphere Configuration Panel](image)
19. Complete the properties for this panel of the wizard:

- **Data Center**: enter your required vSphere data center. Data centers are listed on the **Storage** tab on vSphere.
- **Data Store**: enter the required vSphere data store from your selected data center. Data stores are listed under each data center on the **Storage** tab on vSphere.
- **Resource Pool**: enter the required vSphere resource pool from your selected data center. Resource pools are listed under each data center on the **Hosts and Clusters** tab on vSphere.

  **Note**: If you do not have a resource pool created, then leave the default as `Resources`. This will create a AAA service/Gateway on the default ESX server, provided there is only one ESX server attached to the vCenter. If there are more than one ESX server, then specific Resource Pools will be needed to denote the specific ESX server to deploy on.
- **Appliance Master Template**: provide the default PCS 9.1R1 template. Templates are listed under the data center on the **VMs and Templates** tab on vSphere.

20. Click **Save**.

The wizard closes, and the new *Unregistered* vSphere appliance is added to the list of appliances.

*Figure 23: New Unregistered Controller Appliance*

- The **SDP** setting for the appliance is **AAA service**.

21. Click the **Actions** icon (↑) for the appliance and select **Start Appliance**.

The status of the new appliance goes through a series of states until it successfully running.

- **Unregistered**
- **Creating**
- **Starting**
- **Waiting-on-Certificate**: This status will not clear until you manually complete the configuration of the appliance using its GUI, see [Configuring a AAA Service for SDP](#).
- **Started**
22. (Optional) During the creation of the appliance, you can monitor progress from vSphere's Recent Tasks tab.

Figure 24: vSphere Appliance Creation In Progress

![Figure 24: vSphere Appliance Creation In Progress](image)

Figure 25: vSphere Appliance Creation Complete

![Figure 25: vSphere Appliance Creation Complete](image)

23. Wait until vSphere allocates all IP addresses to the new appliance (see vSphere's Summary tab for a selected appliance).

Note: The appliance is auto-registered. That is, you do not need to manually complete the registration of the appliance from the appliance GUI.

After this process completes, you must configure the vSphere AAA service for SDP, see Configuring a AAA Service for SDP.

Configuring a AAA Service for SDP

The instructions in this section apply to both the SDP controller appliances and SDP gateway appliances on any platform. They must be performed on each such appliance.

To complete the configuration of any AAA service for SDP, you must add the following to it:

- A device certificate, see Adding a Device Certificate to a AAA Service for SDP.
- A CA client certificate chain, see Adding a CA Client Certificate Chain to a AAA Service for SDP.
- A certificate restriction on the admin realms, see Configuring Admin Realms with Client-side Certificate Restrictions.
- An SDP license to enable SDP operations on the appliance, see Adding an SDP License to Enable SDP Operations.
- A secondary administrator account as a fallback when primary Admin account authentication fails, see Creating a Secondary Admin Account.
Adding a Device Certificate to a AAA Service for SDP

To add a Device Certificate to a AAA service for SDP:

1. Log into the GUI for the AAA service as an enterprise administrator.

   ![Figure 26: AAA Service GUI Login](image)

2. Select the **System** menu, and then select **Configuration > Pulse One**.

   The Pulse One **Settings** page appears. This page shows the successful automated registration of the appliance.

   ![Figure 27: Configuration > Pulse One > Settings](image)
3. On the **Settings** page, select the **Certificates** tab.

The Device Certificate page appears with the **Device Certificates** tab open. This tab includes a default device certificate that was added automatically.

**Figure 28: Device Certificate**

![Device Certificate Page]

**Note:** You can optionally delete this default device certificate after you have added your required device certificate.

4. Click **Import Certificate & Key**.

The Import Certificate and Key page appears.

**Figure 29: Import Certificate and Key**

![Import Certificate and Key Page]
5. Identify the import scenario that matches your device certificate:
   - If certificate file includes private key
   - If certificate and private key are separate files
   - Import via System Configuration file

6. Click Browse and select the required file(s) for your scenario.

7. Click Import.
   The device certificate gets listed in the Device Certificate page.

Figure 30: Updated Device Certificate

8. Click the hyperlink for your imported device certificate.
   The Certificate Details page appears.

Figure 31: Certificate Details

9. Under Present certificate on these ports, perform the following:
   - Under Internal Virtual Ports:
     - Click Remove to remove the default device certificate.
     - Click Add to move <Internal Port> into Selected Virtual Ports.
   - Under External Virtual Ports, click Add to move <External Port> into Selected Virtual Ports.
10. Click **Save Changes**.

The Device Certificate page is updated.

**Figure 33: Updated Device Certificate Ports**

11. (Optional) Delete the default device certificate by selecting its check box and clicking **Delete**.

The required device certificate is now present.

You must now add your CA client certificate chain to the AAA service, see [Adding a CA Client Certificate Chain to a AAA Service for SDP](#).
Adding a CA Client Certificate Chain to a AAA Service for SDP

To add a CA Client Certificate Chain to a AAA service for SDP:

1. Select the **System** menu, and then select **Configuration > Certificates > Trusted Client CA**.
   
   The Trusted Client CAs page appears.

   **Figure 34: Trusted Client CAs**

2. Click **Import CA Certificate**.
   
   The Import Trusted Client CA page appears.

   **Figure 35: Import Trusted Client CAs**


4. Under **Import Trusted Client CA?**, click **Import Certificate**.
   
   The CA client certificate chain is added to the list of trusted client CAs.

   **Figure 36: Updated Trusted Client CAs**
Configuring Admin Realms with Client-side Certificate Restrictions

Admin logins require a client certificate that the AAA service is configured to trust - typically, one obtained by enrolling as an SDP client. To implement this, create an admin realm that has a certificate restriction. Admins log in using that realm.

To enable client-side certificate restrictions on the admin realms:

2. Select the Only allow users with a client-side certificate signed by Trusted Client CAs to sign in option.

Figure 37: Certificate Restrictions with Client-side Certificate

You must now add an SDP License to enable SDP operations on a AAA service; (see Adding an SDP License to Enable SDP Operations).

Adding an SDP License to Enable SDP Operations

Pulse One requires an SDP platform license that enables it to be an SDP controller.

Note: if you have installed an SDP license in the Pulse One environment, then the SAML-based Enterprise SSO would be broken.

An administrator can install CONSEC or Named User licenses directly on the AAA service. Pulse One also adds the number of CONSEC or Named User licenses the gateways have.

List of SDP licenses:

- PS-SDP-LIC-1YR
- PS-SDP-LIC-3YR
- PS-SDP-LIC-5YR
- PS-SDP-LIC-1YR-R
- PS-SDP-LIC-3YR-R
- PS-SDP-LIC-5YR-R
To add an SDP license to enable SDP operations on a AAA service:

1. Locate and copy your SDP license key into your clipboard. This takes the general form:
   \[ PS-SDP-xxxx-xxxx : \text{<word> <word> <word> <word> <word> <word>} \]

2. Select the **System** menu, and then select **Configuration > Licensing**.

   The Licensing page appears, with the **Licensing** tab selected. This page shows current licensing on the AAA service. For example:

   **Figure 38: SDP Licensing**
3. Under **Installed license details**, paste your license key and click **Add**.
   After a few minutes, the **SDP** menu option is added to the system menu.

   **Figure 39: System > SDP Menu Option**

4. Select the **System** menu, and then select **SDP**.
   The SDP Overview page appears.

   **Note:** Do not manually select the required **SDP Mode** for the appliance. This will update automatically after Pulse One and the appliance connect.

   **Figure 40: SDP Options**

5. Wait for the **SDP Mode** to automatically set to the correct value (either **Controller** or **Gateway**). This may take several minutes.

   The configuration of the AAA service for SDP is complete.

   After a few minutes, the Appliances page will indicate that the appliance has transitioned from **Waiting-on-Certificate** to **Started**, which indicates that it is now operational.
Creating a Secondary Administrator Account

By default, AAA service creates an admin account with the password you have provided. Using this account, you can manage AAA service via serial console and admin UI console. If this account is locked, then it is not possible to manage AAA service. So, it is recommended to create a secondary admin account.

To create secondary admin account:

In the AAA service serial console, select the option to create administrator username and password.

Or

In the AAA service admin UI console:

2. Click on the Admin user account.
3. In the Users page, select the Users tab.
4. Click New and provide the secondary admin account details.
Creating an SDP Gateway

After you have performed any prerequisite tasks (see Prerequisites for SDP), you can create an SDP gateway as a AAA service on either vSphere or AWS platforms.

To create an SDP gateway:

- Perform either of the following steps:
  - Creating an SDP Gateway on vSphere, OR
  - Creating an SDP Gateway on AWS
- Configuring a AAA Service for SDP.

Note: Once an SDP gateway is added to Pulse One, Pulse One will automatically add the gateway to the controller using the REST API.

Repeat this process until you have all required SDP gateways.

Once you have an SDP controller and all required SDP gateways, you can create all required users on the AAA service (see the Pulse Connect Secure documentation), and then enable application access on the SDP controller, see Managing Application Access on a AAA Service.

Creating an SDP Gateway on vSphere

To create an SDP gateway on vSphere, you perform the same procedure as for the vSphere SDP controller, with the exception of the following gateway-specific step:

- On the Appliance Configuration panel of the registration wizard, you must set the SDP Mode to Gateway.

Figure 41: vSphere Appliance Configuration Gateway

Since the SDP Controller is already created, only the Gateway option appears in SDP Mode.

For the standard procedure to create a virtual AAA service on vSphere, see Creating an SDP Controller on vSphere.
Once the appliance is created, it appears on the Appliances page alongside the SDP controller. For example:

**Figure 42: vSphere Appliance Configuration Gateway**

- The SDP setting for the appliance is *gateway*.
- You can monitor the **Pulse One Status** through the following states:
  - *Unregistered*
  - *Creating*
  - *Starting*
  - *Waiting-on-Certificate*. This status will not clear until you manually complete the configuration of the appliance using its GUI, see [Configuring a AAA Service for SDP](#).
  - *Started*

**Note:** Once an SDP gateway is added to Pulse One, Pulse One will automatically add the gateway to the controller using the REST API.

Once you have an SDP controller and all required SDP gateways, you can create all required users on the AAA service (see the **Pulse Connect Secure documentation**), and then enable application access on the SDP controller, see [Managing Application Access on a AAA Service](#).

## Creating an SDP Gateway on AWS

You can create an SDP gateway on AWS. This process will create the VM appliance and perform all required registration activities on the appliance automatically.

**Note:** This process requires sufficient appliance licensing capacity on Pulse One.

**Note:** You can also create and register a Virtual Machine appliance for vSphere.

Perform the following tasks:

1. Before you begin, you must locate and record the following information:
   - The required Route 53 zones, see [Identifying the Required Route 53 Zones](#).
   - The required VPC ID and Subnet IDs, see [Identifying the Required VPC ID and Subnet IDs](#).
- The required EC2 deployment key, see Identifying the EC2 Deployment Key and AMI ID.

2. You can then create the gateway, see Creating an SDP Gateway on AWS.

3. Finally, configure the AWS AAA service for SDP, see Configuring a AAA Service for SDP.

Identifying the Required Route 53 Zones

Both a private and a public Route 53 zone are required during the creation of a virtual machine AAA service. To locate this information:

1. Log into the AWS Management Console.

2. On the AWS top bar, select the required Region. For example, EU (London).

![Figure 43: AWS Selecting Region](image)

3. On the AWS top bar, click Services and then locate the Network & Content Delivery options.

4. Under Network & Content Delivery, select Route 53.

The AWS Route 53 Management Console appears.

![Figure 44: AWS Route 53 Management Console](image)
5. Select **Hosted Zones**.

The hosted zones panel appears. This lists all domain names (zones) that are available to you.

**Figure 45: AWS Route 53 Hosted Zones**

In the domain name list:

- Zones that have a **Type of Public** have externally-facing (Internet) domain names. The external FQDN that is required when you create the AAA service VM will use the external domain name as a suffix.

- Zones that have a **Type of Private** have internally-facing domain names. The internal FQDN that is required when you create the AAA service VM will use an internal domain name as a suffix.

**Figure 46: AWS Public and Private Zones**

6. Select the required **Public** zone and record its **Domain Name**.

7. Locate the required **Private** zone and record its **Domain Name**.

You can then perform any remaining preparations, and then continue to create and register the AAA service virtual machine on AWS.

**Identifying the Required VPC ID and Subnet IDs**

A VPC identifier is required during the creation of a virtual machine AAA service. To locate this information:

1. Log into the AWS Management Console.

2. On the AWS top bar, select the required **Region**.

3. On the AWS top bar, click **Services** and then locate the **Network & Content Delivery** options.
4. Under **Network & Content Delivery**, select **VPC**.

The AWS VPC Dashboard appears.

**Figure 47: AWS VPC Dashboard**

5. Select **Your VPCs**

A list of available VPCs appears.

**Figure 48: AWS Available VPCs**

6. Locate the required VPC and record its **VPC ID**. For example:

**Figure 49: AWS VPC ID**

7. In the **Filter by VPC** filter, select the required VPC. For example:

**Figure 50: AWS Select VPC**
8. Click Subnets.
A list of all subnets in the selected VPC appears.

**Note:** This list must include three different subnets that are in the same Availability Zone. Each will be used for one of the standard PCS interfaces in a later procedure (see Creating an SDP Gateway on AWS). The interfaces requirements are:

- **Internal interface** - This must be a private subnet.
- **External Interface** - This must be a public subnet.
- **Management Interface** - This can be either a public or private subnet, depending on your requirements.

Where the required subnets do not exist, you must create them before proceeding.

9. Select a public subnet and record its Subnet ID from the bottom panel. For example:

**Figure 51: AWS Select Public Subnet**

![Figure 51: AWS Select Public Subnet](image)

The public subnet will be used for the External interface or Management interface of the Gateway at a later procedure.

10. Select a private subnet (in the same Availability Zone as step 9) and record its Subnet ID from the bottom panel. This subnet be used for the external interface of the AAA service in a later procedure.

11. Select a third subnet (either private or public, and in the same Availability Zone as step 9) and record its Subnet ID from the bottom panel. This subnet be used for the management interface of the AAA service in a later procedure.

You can then perform any remaining preparations, and then continue to create and register the AAA service virtual machine on AWS.

**Identifying the EC2 Deployment Key and AMI ID**

An EC2 key pair (deployment key) and an AMI ID are required during the creation of a virtual machine AAA service. To locate this information:

1. Log into the AWS Management Console.
2. On the AWS top bar, select the required Region.
3. On the AWS top bar, click Services and then locate the Compute options.
4. Under **Compute**, select **EC2**.

The AWS EC2 Dashboard appears, showing **Key Pairs**.

**Figure 52: AWS EC2 Dashboard**

5. In the **Resources** panel, click **Key Pairs**.

A list of defined key pairs appears.

**Figure 53: AWS EC2 Key Pairs**

6. Select the required key pair and record its **Key pair name** from the bottom panel. This name is used as the “deployment key” during installation. For example:

**Figure 54: AWS Select EC2 Key Pair**
7. On the EC2 dashboard menu, under **Images** select **AMIs**.

A list of defined AMIs appears. For example:

**Figure 55: AWS EC2 AMIs**

8. Select the required AMI and record its **AMI-ID** from the bottom panel. For example:

**Figure 56: AWS EC2 AMIs**

You can then perform any remaining preparations, and then continue to create and register the SDP gateway on AWS.

**Creating an SDP Gateway on AWS**

Once you have identified all required information, you can start the process to create an SDP gateway on AWS:

1. Start Pulse One.

2. Click the **Appliances** menu and then the **Appliances** tab.

   The **Appliances** tab displays all current appliances.
3. Click **Add Appliance**.

   The Add Appliance wizard starts.

   **Figure 57: Add Appliance**

4. Select **Create virtual appliance in Amazon Web Services** and click **Next**.

   The AWS Credentials panel of the wizard appears.

   **Figure 58: AWS Credentials**

5. Complete the properties for this panel of the wizard.

   For the first use of this wizard:
   - For **Account**, select **Add New**.
   - Enter your AWS **Access Key** and **Secret Key**.

   For later uses of the wizard, select the required **Account**. The credentials for this are stored, and do not need to be entered.
6. Click **Next**.

The Appliance Configuration panel of the wizard appears.

**Figure 59: Appliance Configuration**

7. Enter the **Appliance Name**. This will be the displayed name in the list of appliances and will also be used to automatically populate the **Internal FQDN** and **External FQDN** properties on subsequent wizard panels.

8. Select **Gateway** as SDP Mode.

9. Specify additional information for the appliance:
   - **A Company Name**.
   - Note that the **SDP License Auth Code** field currently does not use the licenses added here.
   - The **Appliance Username, Password (and Confirm Password)** for a required user on the appliance. This user will be created once the appliance is created.
10. Click **Next**.

The **Appliance Network Configuration** panel of the wizard appears.

**Figure 60: Appliance Network Configuration: Servers**

11. Specify the **Primary DNS** and the **Secondary DNS** for your network.

   ![Image](image_url)

   **Note:** The displayed values are examples, and not defaults.

12. Expand the **Internal Network Settings** panel.

   ![Image](image_url)

13. In the **Internal Network Settings**:

   - For the **Hosted Zone**, enter the internal domain name (internal Route 53 hosted zone) for your appliance. See **Identifying the Required Route 53 Zone**.

   ![Image](image_url)

   **Note:** When you shift focus away from this property, the internal **Hosted Zone** setting is displayed as a suffix to **Internal FQDN**.
For the Internal FQDN, complete the FQDN by adding a unique appliance identifier to the left-hand side of the internal domain name in this field. Typically, you will specify the Appliance Name you specified in the Appliance Configuration dialog, and the internal Hosted Zone is used as a suffix.

14. Expand the External Network Settings panel.

![Figure 62: Appliance Network Configuration: External Network Settings](image)

15. In the External Network Settings:
   - For the Public Domain Name, enter the external domain name (external Route 53 hosted zone) for your appliance. See Identifying the Required Route 53 Zone.
   
   ‣ Note: When you shift focus away from this property, the external Hosted Zone setting is displayed as a suffix to External FQDN.

   - For the External FQDN, complete the FQDN by adding a unique appliance identifier to the left-hand side of the external domain name in this field. Typically, you will specify the Appliance Name you specified in the Appliance Configuration dialog, and the external Hosted Zone is a suffix.
16. Expand the **Management Network Settings** panel.

**Figure 63: Appliance Network Configuration: Management Network Settings**

17. (Optional for SDP Gateway) In the **Management Network Settings**:
   - For **Management Domain Name**, enter a name for the AWS network.
     
     **Note:** When you shift focus away from this property, the **Management Domain Name** setting is displayed as a suffix to **Management FQDN**.

   - For the **Management FQDN**, complete the FQDN by adding a unique appliance identifier to the left-hand side of the external domain name in this field. Typically, you will specify the **Appliance Name** you specified in the **Appliance Configuration** dialog, and the **Management Domain Name** is a suffix.

18. Click **Next**. The **AWS Configuration** panel of the wizard appears.

**Figure 64: AWS Configuration**
19. Specify the following properties:

- **Amazon Machine Image (AMI)** is the AMI ID that you identified in Identifying the EC2 Deployment Key and AMI ID.
- **VPC ID** is the value that you identified in Identifying the Required VPC ID and Subnet IDs.
- **Region** is a drop-down list from which you select your specific region.
- **Private Subnet ID, Public Subnet ID, and Management Subnet ID** are the three subnet IDs that you identified in Identifying the Required VPC ID and Subnet IDs.
- **Deployment Key** is the key pair that you identified in Identifying the EC2 Deployment Key and AMI ID.

20. Click **Save**.

The wizard closes, and the new *Unregistered* AWS appliance appears on the Appliances page alongside the SDP controller.

**Figure 65: AWS Appliance Configuration Gateway**

The **SDP** setting for the appliance is **gateway**.

You can monitor the **Pulse One Status** through the following states:

- **Unregistered**
- **Creating**
- **Starting**
- **Waiting-on-Certificate**. This status will not clear until you manually complete the configuration of the appliance using its GUI, see Configuring a AAA Service for SDP.
- **Started**

**Note:** Once an SDP gateway is added to Pulse One, Pulse One will automatically add the gateway to the controller using the REST API.
(Optional) Wait until the appliance reaches a Created state, then go to the **EC2 Dashboard** in AWS and view **Instances**. The new appliance is listed and reports a **Status Check** of Initializing.

**Figure 66: AWS Initializing Appliance**

![AWS Initializing Appliance](image)

**Note:** The appliance is auto-registered. That is, you do not need to manually complete the registration of the appliance from the appliance GUI.

After this process completes, you must configure the AWS SDP gateway for SDP, see [Configuring a AAA Service for SDP](#).

Once you have an SDP controller and all required SDP gateways, you can create all required users on the AAA service (see the *Pulse Connect Secure* documentation), and then enable application access on the AAA service, see [Managing Application Access on a AAA Service](#).

### Adding an Existing PCS Appliance

Once Pulse One is installed and configured, you can register one or more existing PCS appliances.

To register an existing appliance:

1. Start Pulse One.
2. Click the **Appliances** menu and then the **Appliances** tab.
   
   The **Appliances** tab displays all current appliances.
3. Click **Add Appliance**.
   
   The **Add Appliance** dialog box appears.

   **Figure 67: Add Appliance**

   ![Add Appliance](image)

4. Select **Register existing appliance** and click **Next**.
   
   The **Register Appliance** dialog appears.
5. Enter the required **Name** for the appliance. For example: `appliance.pcs`.

6. Enter the admin user interface address as the **Appliance URL**.

7. (Optional) If you want the appliance to support Device Management Interface (DMI) software upgrades directly from Pulse One:
   - For **IP Address**, specify the IP Address on which the appliance is configured to receive DMI requests. This is either the internal interface or the management interface.
   - For **Port**, specify the port on which the appliance is configured to receive DMI requests. Typically, this is 830.
   - Specify an admin **Username** and **Password** for the appliance. This will be used to receive DMI requests.

8. Click **Save**.

   A dialog displays the required **Registration Host** and a **Registration Code**.

---

**Figure 69: Registration Required**
9. Record the **Registration Host** and **Registration Code** and close the dialog.

10. Switch to the appliance application (for example, PCS) and enter the **Registration Host** and the **Registration Code** in the appliance's panel, see [Completing Registration of an Appliance](#). When the auto-registration process is complete, Pulse One console displays the appliance status as **Completed** in the appliances list.

11. Click the Actions icon and select **Configure SDP**.

12. In the Configure FQDN window, type the appliance's External FQDN and click **Configure**.

    **Figure 70: Configure FQDN**

13. When the configuration is complete, Pulse One console displays the appliance status as **Configured** in the appliances list.

    **Figure 71: Appliance with Configured Status**

14. When the configuration is complete, SDP controller pushes sdp_enrollment role and sdp_no_cert to AAA service. The sdp_no_cert allows user to access L7 applications via browser.

    **Figure 72: Rules with sdp_enrollment and sdp_no_cert Rules**
Completing Registration of an Appliance

To complete registration of an appliance in Pulse Connect Secure:

1. Log into the GUI of the PCS appliance.
2. Select the System > Configuration > Pulse One > Settings tab.
3. Enter the Registration Host and Registration Code.
4. Select Preferred network interface as External Port.

Editing Appliance Information

To edit appliance information:

1. Start Pulse One.
2. Click the Appliances menu and then the Appliances tab.
   
   The Appliances tab displays all current appliances.
3. Select the required appliance from the list and click its Actions icon ( ).
4. From the menu options, select Edit Appliance Info.
5. In the Edit Appliance Info dialog, make the required changes.

   Note: If you want the Launch Appliance UI option to be available on the Actions menu for the appliance, specify the Appliance URL. This URL typically ends with “/admin”.

6. Click Save to update the appliance.
Managing Application Access on a AAA Service

Once SDP is fully enabled on Pulse One, the following tasks are required to manage application access on the AAA service:

- Creating a Resource Profile on a AAA Service
- Adding an Application to an SDP Gateway
- REST API Commands

For full details of all PCS operations, see the Pulse Connect Secure documentation.

Creating a Resource Profile on a AAA Service

A resource profile contains the resource policies, role assignments, and end-user bookmarks required to provide access to an individual resource. You need to create separate roles for L3 and L4/L7 client connections.

AAA service supports the following resources:

- Web applications
- HTML5 access
- Files
- L3 applications
- VPN tunneling
- WSAM Client application

**Note:** When L4 WSAM Client application is pushed from SDP controller to SDP gateway, L3 ACL/Split Tunneling policies will not be created automatically in SDP gateway.

An administrator can apply certificate and host checker restrictions to specific roles. A device gets limited resource access if the device fails the certificate restrictions or host checker policies.

For details on creating resource profile roles, policies, bookmarks on a AAA service, refer to the Resource Profiles section in the Pulse Connect Secure Administration Guide.

Adding an Application to an SDP Gateway

Each application that is required on an SDP gateway must be pushed down to the gateway from the SDP controller.

To add an application to an SDP gateway:

1. Log into the GUI for the SDP controller as an administrator. On successful authentication, Pulse One redirects to AAA service authentication.
2. On successful log into AAA service, select the AAA tab for AAA service.
3. Select the System menu, and then select SDP > Applications > New.
The Publish Applications page appears.

**Figure 72: SDP Publish Applications**

4. Enter an **Application name**.
5. Select the required **Gateway Location**.
6. Select the required **Resource Type**.
7. Select the required **Resource Profile**.
8. Click **Save Changes**.
   
   The application is then pushed to the selected gateway.

**REST API Commands**

**Get Application List through REST**

```bash
curl -s -ku xGtzaTZrz7LJpm22+kTz6p4KDwT0fwk4pGRz+737I=: https://10.96.144.125/api/v1/configuration/system/sdp/applications
{
  "application": [
    {
      "href": "/api/v1/configuration/system/sdp/applications/application/OutlookApp",
      "name": "OutlookApp"
    },
    {
      "href": "/api/v1/configuration/system/sdp/applications/application/samdestapp",
      "name": "samdestapp"
    }
  ]
}```
Publish Application through REST

Publish Web profile

curl -s -ku xGtzaTZrz7LJp22+kTz6p4KDuT0fwk4pGRz+r73q7l=:
https://10.96.144.125/api/v1/configuration/system/sdp/applications/application
-X POST -H "Content-Type:
application/json" -d '{"name": "OutlookApp", "gateway": "bangalore", "web": {"profile": "outlook"}}'

{  
  "result": {  
    "info": [  
      {  
        "message": "Operation succeeded without warning or error!"  
      }  
    ]  
  ]  
}
Publish SAM Destinations Profile

curl -s -ku xGtzaTzrz7LjPm22+kTz6p4KDuT0fwk4pGRz+73q7I=:https://10.96.144.125/api/v1/configuration/system/sdp/applications/application -X POST -H "Content-Type: application/json" -d "{"name": "samdestapp", "gateway": "bangalore", "wsam": {"profile": "samdestLinux"}}"

{
"result": {
"info": [
{
"message": "Operation succeeded without warning or error!"
}
]
}
}

Publish HTML5 Access Profile

curl -s -ku xGtzaTzrz7LjPm22+kTz6p4KDuT0fwk4pGRz+73q7I=:https://10.96.144.125/api/v1/configuration/system/sdp/applications/application -X POST -H "Content-Type: application/json" -d "{"name": "html5app", "gateway": "Bangalore", "html5": {"profile": "RDP Server"}}"

{
"result": {
"info": [
{
"message": "Operation succeeded without warning or error!"
}
]
}
}
**Publish Windows File Browsing Profile**

```bash
curl -s -ku xGtzaTZr7LjPm22+kTz6p4KDuT0fwk4pGRz+/73q7I=:
https://10.96.144.125/api/v1/configuration/system/sdp/applications/application -X POST -H "Content-Type: application/json" -d '{"name": "fbapp", "gateway": "Bangalore", "windows-files": {"profile": "windows_file_share"}}'

{  
"result": {  
  "info": [  
    {  
      "message": "Operation succeeded without warning or error!"
    }  
  ]  
}
}
```

**Publish VPN Tunneling Profile**

```bash
curl -s -ku xGtzaTZr7LjPm22+kTz6p4KDuT0fwk4pGRz+/73q7I=:

{  
"result": {  
  "info": [  
    {  
      "message": "Operation succeeded without warning or error!"
    }  
  ]  
}
}
```

**Publish VPN ACL**

```bash
curl -s -ku xGtzaTZr7LjPm22+kTz6p4KDuT0fwk4pGRz+/73q7I=:

{  
"result": {
```

© 2019 by Pulse Secure, LLC. All rights reserved
"info": [
  {
    "message": "Operation succeeded without warning or error!"
  }
]

Delete Application

Example: Delete an application with application name as 'html5app'

curl -s -ku xGtzaTZrz7LjPm22+kTz6p4KDuT0fwk4pGRz+/737I=: https://10.96.144.125/api/v1/configuration/system/sdp/applications/application/html5app -X DELETE
Accessing the End User Portal on Pulse One

After operational SDP controller/gateways are deployed from Pulse One, any non-admin attempt to access Pulse One is redirected to the SDP controller. For example, in a browser:

```plaintext
https://<pulse_one_server>/login
```

This will result in the Pulse One server redirecting to the SDP controller.

Note: It is strongly recommended to log into the AAA Service via Pulse One. Avoid logging into the AAA service directly unless directed by Pulse Secure support.

Figure 73: Pulse One Login Redirects to SDP Controller

Note: Admin access to Pulse One is unaffected: `https://<pulse_one_server>/admin`

Once you are logged in to the SDP controller, you are directed to the SDP Controller portal. This page lists any published apps, see Adding an Application to an SDP Gateway.

Figure 74: SDP Controller

When an app is selected, the app is accessed on the gateway to which it is published.
SDP Enabled Pulse Desktop Client

From 9.1R1 onwards, SDP enabled Pulse Desktop Client is available for only Windows. SDP enabled Pulse Desktop Client for macOS will be available in future releases.

Pulse Desktop Client is an application which provides functionality for both SDP enabled and classic Pulse Desktop Client features. At one point of time, either classic PDC connection or SDP enabled PDC connection can be established.

The following scenario describes the behavior of SDP enabled PDC connection and classic PDC connections concurrency.

**Scenario** – SDP_CONN and Classic_CONN Concurrency

In this scenario, we have one classic PDC connection named as **Classic_CONN** and one SDP enabled PDC connection named as **SDP_CONN**.

If the user is connected to classic PDC connection **Classic_CONN**, and the user disconnects classic PDC connection **Classic_CONN** then SDP enabled PDC connection **SDP_CONN** can be established. Refer to the following figures:

Figure 75: SDP_CONN
Figure 76: Classic_CONN
SDP Enabled Pulse Desktop Client Onboarding

This section describes how the SDP enabled Pulse Desktop Client establishes a connection to the SDP controller for the first time (onboarding) and how that connection is maintained.

Note: SDP onboarding is not supported via Pulse Secure Command-line Launcher.

Note: SDP onboarding will not support Always-on VPN.

Following are the two deployment scenarios to understand the behavior of SDP enabled Pulse Desktop Client onboarding.

Scenario 1 – User based Onboarding

Prerequisite - Pulse Desktop Client 9.1R1 is installed.

Pulse Desktop Client 9.1R1 is installed, the administrator configures the onboarding URL and the user does the onboarding.

1. Launch Pulse Desktop Client 9.1R1 and click Add Connection.

   The following screen appears:

   **Figure 77: Add Connection**

   ![Add Connection Screen](image)

2. Enter the required information:
   - **Type** - Select the type as SDP from the drop-down box.
   - **Name** - Enter the name of the SDP connection.
Server URL - Enter the server URL directing to SDP enrollment URL.

The following screenshot displays SDP connection name as **sdp_connection** and server URL as *aaa.p1clienta.pdcteam.com/enroll*.

**Figure 78: SDP – Connection Details**

3. Click the **Add** button. SDP connection named as **sdp_connection** gets added.

The following screen appears:
4. Click the **Connect** button.

   The following authentication window appears:

   **Figure 80: Authentication Window**

5. Enter the **User Name** and the **Password**.

6. Click the **Connect** button.

   The following screen appears:
The authenticated user is getting on boarded or getting enrolled. At this point, the user is connected to Pulse Workspace.

**Figure 82: Onboarding Status – Connected**

The authenticated user is onboarded successfully, and the user is enrolled to the SDP controller now.

7. If a single certificate is installed, SDP enabled PDC will automatically take the certificate from user’s certificate store.

If two certificates are installed, the user needs to select the certificate as shown in the below screen:
8. Click the **Cancel** button if the user wants to connect to the SDP controller later.

Or click the **Connect** button to connect to the SDP controller.

The following screens appear.

**Figure 84: User authentication to SDP Controller**
The SDP controller connection (sdp_connection) is established, and the SDP gateways connections are also established automatically in the backend.

**Note:** User can edit the SDP connection name, but not the SDP connection server URL.

Right-click on sd_connection. The following screen appears:
Figure 86: Advanced Connection Details

Click **Advanced Connection Details**. The following screen appears:

Figure 87: Advanced Connection Details
9. Click the **Home** button.

   The following screen appears:

   **Figure 88: Home Screen**

   ![Home Screen]

   External browser window is launched and loads the End User Portal.

10. Click **Disconnect** button to disconnect the SDP enabled PDC connection (sdp_connection).

    Once the user disconnects the connection, the user automatically gets logged out from SDP gateways along with the SDP controller.

### Scenario 2 – Browser based Onboarding

Browser based onboarding is done if Pulse Desktop Client is not installed. Follow the below mentioned steps to perform browser-based onboarding.

1. Log into the Pulse One console.
   
   The following screen appears:

   **Figure 89: Enroll in SDP Window**

   ![Enroll in SDP Window]

2. Click **Enroll in SDP**. The following screen appears:

   Type AAA service URL in the browser. For example, *aaa.p1clienta.pdcteam.com/enroll*
3. Enter the user name and the password.
4. Click **SIGN IN**. The following screen appears:

Figure 91: Welcome Page
Figure 92: Pop-up Window

Internet Explorer Security

A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer’s Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: PulseExt.exe
Publisher: Pulse Secure, LLC

☐ Do not show me the warning for this program again

Allow  Don’t allow

5. Click **Allow**. SDP enabled PDC connection (sdp_connection) is already created in Pulse Desktop Client. The following screen appears:

Figure 93: Connection established

6. Click **Connect**. Follow the steps from Step-5 onwards in the Scenario 1 – User based Onboarding.

**Note:** For the SDP controller connection, the Pulse Desktop Client does not support machine authentication and credential provider authentication.
Multiple Tunnels Support for SDP Enabled Pulse Desktop Client

Globally, all enterprises are adapting cloud technologies in some form. Enterprises choose public cloud or private cloud, SaaS services and/or co-locate their data center based upon their needs and business strategies. Eventually, this leads to a Hybrid-IT type of deployment where there is more than one location, where the enterprise resources such as business applications, data bases, IT systems are deployed. Employees and partners of these enterprises must access these business applications and data from anywhere, anytime irrespective of where these resources are deployed.

The end users (employees and partners) are expected to connect to these applications spread across multiple locations, which are protected by Secure Access solutions such as Pulse SDP. End users expect a very seamless experience in accessing the applications or when switching between applications for their work. So, it is very critical to provide capability on the client side to access multiple applications deployed across multiple locations (public/private cloud, SaaS) in a seamless manner.

Pulse Desktop Client with SDP capability is now enabled to support multiple tunnels to Gateways deployed in multiple locations. With this capability, user needn't worry about switching between gateways to access the applications. All applications can be accessed at the same time in a seamless manner for providing the best end user experience and productivity.

SDP enabled Pulse Desktop Client will be able to handle multiple tunnels simultaneously. Multiple tunnels must co-exist with at least one Layer 3 tunnel.

User connects to the SDP controller manually, the connections to the SDP gateways are established automatically by SDP enabled PDC and the tunnel will be created.

After authentication, SDP enabled Pulse Desktop Client receives FQDN policies, gateway URLs from the SDP controller. After receiving policies from SDP controller, SDP enabled PDC establishes one Layer 3 and multiple PSAM tunnels based on the SDP controller configuration.

---

**Note:**
- For Windows, single L3 tunnel and multiple PSAM tunnels are supported.
- For macOS, multiple L3 tunnels are supported.

**Note:**
- FQDN (Include policy) and IP address ranges (include policy) are supported for both Layer 3 tunnel and PSAM tunnel.
- L3 based FQDN Split Tunneling feature with PSAM coexistence is not supported.
- FQDN policies should be unique across the gateways, if FQDN policies are not unique the tunnel gets established with first match of gateway.

**Note:** SRV query and Netbios query are not supported.
The following section describes configuring one L3 and multiple PSAM tunnel configurations.

**Configuring L3 Split Tunnel for an SDP Gateway**

**Prerequisites**

The following are the prerequisites for configuring L3 Split Tunnel for an SDP Gateway:

- SDP L4 gateways IP addresses should be excluded from L3 gateway.
- SDP Controller (AAA) and Pulse one IP addresses should be excluded from L3 gateway.
- L3 full tunnel is not supported in SDP mode.

**Enabling L3 Split Tunneling Connection Profile**

To configure a L3 split tunnel to an SDP gateway:

1. Log into the GUI for the SDP controller as an administrator.
2. Select the **System** menu, and then select **SDP > Applications > New**.

   ![Figure 94: Publish Applications – Enabling L3 Split Tunnel Connection Profile](image)

   - **Application name**
   - **Gateway Location**: `sdpgw1`
   - **Resource type**: **VPN Connection Profiles**
   - **Resource profile**: `agent`

3. Enter the **Application name**.
4. Select the required **Gateway Location**.
5. Select the **Resource type** as **VPN Connection Profiles**.
6. Select the required **Resource profile**.
7. Click **Save Changes**.
The application is then pushed to the selected gateway.

**Defining L3 Split Tunneling Policies**

1. Select the **System** menu, and then select **SDP > Applications > New**.

The following Publish Applications page appears:

![Publish Applications](image)

**Figure 95: Publish Applications – Defining L3 Split Tunneling Policies**

2. Enter an **Application name**.
3. Select the required **Gateway Location**.
4. Select the **Resource type** as **Split Tunneling Networks**.
5. Select the required **Resource profile**.
6. Click **Save Changes**.

The application is then pushed to the selected gateway.

**Configuring PSAM Tunnel for an SDP Gateway**

**Client Applications**

1. Select the **System** menu, and then select **SDP > Applications > New**.

The following Publish Applications page appears:
Figure 96: Publish Applications – Client Applications

2. Enter an **Application name**.
3. Select the required **Gateway Location**.

   ![Note: PSAM Gateway Location should be different from L3 Gateway Location.]

4. Select the required **Resource Type**.
5. Select the **Resource Profile** as **SAM/Client Applications**.
6. Click **Save Changes**.

   The application is then pushed to the selected gateway.

**WSAM Destinations**

1. Select the **System** menu, and then select **SDP > Applications > New**.

   The following Publish Applications page appears:
2. Enter an **Application name**.
3. Select the required **Gateway Location**.
4. Select the **Resource type** as **SAM/WSAM Destinations**.
5. Select the required **Resource profile**.
6. Click **Save Changes**.

The application is then pushed to the selected gateway.

The following table describes different scenarios of L3 and multiple Pulse SAM tunnel w.r.t to SDP enabled Pulse Desktop Client:

**Table 1: Scenarios of L3 and multiple Pulse SAM tunnel**

<table>
<thead>
<tr>
<th>Tunnel Type</th>
<th>Configured Rules</th>
<th>Accessed by</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>L3+Multiple Pulse SAM</td>
<td>1. L3 ST enabled with PSAM gateways excluded.</td>
<td>1. User Access &lt;google.com&gt;</td>
<td>1. As per rule the google.com will be tunneled via SA1.</td>
</tr>
<tr>
<td></td>
<td>2. WSAM destination with &lt;google.com, amazon.com&gt; to SA1.</td>
<td>2. User Access &lt;amazon.com&gt;</td>
<td>2. As amazon.com exists in both policies, but SA1 will evaluate the</td>
</tr>
<tr>
<td></td>
<td>3. User connected SA1 and then SA2</td>
<td></td>
<td>policy first. Rest of the traffic goes via L3 tunnel.</td>
</tr>
<tr>
<td></td>
<td>4. Chrome application with &lt;youtube.com&gt; to SA1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. WSAM destination with &lt;youtube.com&gt; to SA2.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2019 by Pulse Secure, LLC. All rights reserved
<table>
<thead>
<tr>
<th>Tunnel Type</th>
<th>Configured Rules</th>
<th>Accessed by</th>
<th>Rule</th>
</tr>
</thead>
</table>
| L3+Multiple Pulse SAM | L3 ST enabled with PSAM gateways excluded.  
WSAM destination with <*.com> to SA1  
WSAM destination with <youtube.com> to SA2 | User access with youtube.com                   | SA2 is selected as its longest domain match.                         |
| L3+Multiple Pulse SAM | L3 ST enabled with PSAM gateways excluded.  
10.209.122.68/255.255.240.0 :3389 for SA1  
10.209.112.0/255.255.240.0 :3389 for SA2 | User access with rdp using 10.209.122.168 IP address. | SA1 is selected because of the longest prefix length.                |
| L3+Multiple Pulse SAM | L3 ST enabled with PSAM gateways excluded.  
[fdo1:2001:366:64::64] for SA1  
SDP Enabled Pulse Desktop Client Configuration Settings

To launch the configuration page, select Users > Pulse Secure Client > Connections.

The following table, and Figure 98, Figure 99 and Figure 100 describe SDP enabled Pulse Desktop Client configuration settings.

Table 2: SDP Enabled Pulse Desktop Client Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Editable/Non-Editable/Invalid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow saving logon information</td>
<td>If you select this check box, users have the option of saving their credentials.</td>
<td>Editable</td>
</tr>
<tr>
<td>Allow user connections</td>
<td>Select the check box to allow user to add connection through the Pulse client interface.</td>
<td>Invalid</td>
</tr>
<tr>
<td>Always-on Pulse Client</td>
<td>Prevent the end users from circumventing Pulse connections. This option disables all configuration settings that allow the end user to disable or remove Pulse connections, service or software.</td>
<td>Invalid</td>
</tr>
<tr>
<td>Display Splash Screen</td>
<td>Uncheck this check box to hide the Pulse splash screen which normally appears when the Pulse client starts.</td>
<td>Editable</td>
</tr>
<tr>
<td>Dynamic certificate trust</td>
<td>Determines whether users can opt to trust unknown certificates. If you select this check box, a user can ignore warnings about invalid certificates and connect to the target Pulse server.</td>
<td>Editable</td>
</tr>
<tr>
<td>Dynamic connections</td>
<td>Allows new connections to be added automatically to a Pulse Secure client when the user logs into a Pulse server through the server’s Web portal, and then starts Pulse though the Web portal interface.</td>
<td>Invalid</td>
</tr>
<tr>
<td>EAP Fragment Size</td>
<td>Maximum number of bytes in EAPoL message from the client for 802.1x connections.</td>
<td>Editable</td>
</tr>
<tr>
<td>Enable captive portal detection</td>
<td>Select this check box to detect the presence of a captive portal hotspot. It can be applied only to Pulse Connect Secure and Pulse Policy Secure (L3) connections.</td>
<td>Non-Editable</td>
</tr>
<tr>
<td>Enable embedded browser for authentication</td>
<td>When this option is enabled, Pulse uses an embedded browser for web authentication, rather than external browser.</td>
<td>Non-Editable</td>
</tr>
<tr>
<td>Enable embedded browser for captive portal</td>
<td>When this option is enabled, Pulse uses an embedded web browser that the end user can use to traverse captive portal pages and to gain network connectivity for establishing a VPN connection. This applies only when captive portal detection is enabled.</td>
<td>Non-Editable</td>
</tr>
<tr>
<td>FIPS mode enabled</td>
<td>Enable FIPS mode communications for all Pulse connections in the connection set. The Federal Information Processing Standard (FIPS) defines secure communications for the U.S. government. When a Pulse connection is operating in FIPS mode, FIPS On appears in the lower corner of the Pulse client interface.</td>
<td>Editable</td>
</tr>
<tr>
<td>Prevent caching smart card PIN</td>
<td>Enabling this field will allow system administrators to prevent smart card PIN values from being cached. This feature is applicable only to Windows.</td>
<td>Editable</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Editable/Non-Editable/Invalid</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>VPN only access</td>
<td>When the Pulse client connects to Pulse Connect Secure having lock down mode enabled, it will enable lock-down mode and block network if VPN is not in connected state.</td>
<td>Invalid</td>
</tr>
<tr>
<td>Wireless suppression</td>
<td>Disables wireless access when a wired connection is available. Wireless suppression occurs only when the wired connection is connected and authorized.</td>
<td>Editable</td>
</tr>
<tr>
<td>Allow user to override connection policy</td>
<td>Allows a user to override the connection policy by manually connecting or disconnecting. Typically, you leave this option selected to make sure that a user can establish a connection under all conditions. If you disable this check box, the user cannot change the endpoint's connection status, suspend/resume a connection to Pulse Connect Secure or shut down Pulse Secure client.</td>
<td>Editable</td>
</tr>
<tr>
<td>Lock down this connection</td>
<td>Network access is limited until this connection is established. This option is available only when the Always-on Pulse Client option or VPN only access option on the connection is enabled.</td>
<td>Invalid</td>
</tr>
<tr>
<td>Enable stealth mode on this connection</td>
<td>When this option is enabled, user will not be able to see and control the established connection through the Pulse Client UI. User or machine authentication will happen seamlessly without any user interaction.</td>
<td>Invalid</td>
</tr>
<tr>
<td>Show stealth connection to users</td>
<td>When this option is enabled, user will be able to see the Stealth mode connection in Pulse UI. User will be able to see only the connection status in Pulse Tray icon and an option to view Advanced Connection details. User will not be able to control any actions.</td>
<td>Invalid</td>
</tr>
<tr>
<td>Support Remote Access (Connect Secure) or LAN Access (Policy Secure) on this connection</td>
<td>Uncheck this check box if the connection is not used for Connect Secure or Policy Secure services.</td>
<td>Invalid</td>
</tr>
<tr>
<td>Enable Pulse Collaboration integration on this connection</td>
<td>You can disable this check box and use the connection for accessing Pulse Collaboration meetings only by also selecting Enable Pulse Collaboration integration on this connection.</td>
<td>Invalid</td>
</tr>
<tr>
<td>Connect to URL of this server only</td>
<td>Specifies whether the endpoint connects to this Pulse server exclusively or if it can connect to the any of the servers listed in the list of connection URLs. Disable this check box to enable the List of Connection URLs.</td>
<td>Editable</td>
</tr>
<tr>
<td>List of connection URLs</td>
<td>Allows you to specify a list of Pulse servers (Pulse Policy Secure or Pulse Connect Secure) for this connection. The Pulse client attempts to reach each server in the list, in the order listed, until it succeeds. You can specify up to 8 Pulse servers.</td>
<td>Editable</td>
</tr>
<tr>
<td>Attempt most recently connected URL first</td>
<td>If you have specified a list of connection URLs, you can select this check box to have the Pulse client always attempt the most recent successful connection. If that connection is not successful, Pulse then starts at the top of the list. The most recently connected URL is saved across reboots.</td>
<td>Editable</td>
</tr>
<tr>
<td>Randomize URL list order</td>
<td>If you have specified a list of connection URLs, select this check box to have the Pulse client ignore the order in which the servers are listed. You can select this option to spread the connection load across multiple Pulse servers.</td>
<td>Editable</td>
</tr>
<tr>
<td>Use Desktop Credentials</td>
<td>If you select this check box, then the system login credentials will be cached and used for this connection.</td>
<td>Editable</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Editable/Non-Editable</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Enable Automatic Client Certificates Selection</td>
<td>This option uses a proprietary certificate ranking algorithm to choose the most suitable client certificate.</td>
<td>Editable</td>
</tr>
</tbody>
</table>

**Specify mode**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Editable/Non-Editable</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Enables user authentication.</td>
<td>Non - Editable</td>
</tr>
<tr>
<td>Machine</td>
<td>Enables machine authentication, which requires that Active Directory is used as the authentication server and that machine credentials are configured in Active Directory. A machine connection is, by default, an automatic connection.</td>
<td>Non - Editable</td>
</tr>
<tr>
<td>Machine or User</td>
<td>Enables machine authentication for the initial connection. After user authentication, the machine authentication is dropped. When the user logs out, the machine authentication connection is restored.</td>
<td>Non - Editable</td>
</tr>
</tbody>
</table>

**Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Editable/Non-Editable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect automatically</td>
<td>Connections are attempted when the conditions specified in the location awareness rules are true and disconnected when the conditions are no longer true.</td>
<td>Invalid</td>
</tr>
</tbody>
</table>

**Note**: This configuration setting is not recommended for the connection.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Editable/Non-Editable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnect at Session Timeout or Deletion</td>
<td>If this option is enabled, user - initiated sessions automatically attempt to reconnect upon a session timeout or deletion. If this option is disabled, then user - initiated sessions remain disconnected upon a session timeout or deletion.</td>
<td>Editable</td>
</tr>
<tr>
<td>Enable pre-desktop login (Credential Provider)</td>
<td>Enables Pulse client interaction with the credential provider software on the endpoint. The user credentials are used to establish the authenticated Pulse connection to the network, login to the endpoint, and login to the domain server.</td>
<td>Invalid</td>
</tr>
<tr>
<td>Location Awareness Rules</td>
<td>For Connect Secure or Policy Secure (L3) connections that are set to have the connection established automatically, you can define location awareness rules that enable an endpoint to connect conditionally.</td>
<td>Invalid</td>
</tr>
</tbody>
</table>

**User Connection Preferences**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Editable/Non-Editable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred User Realm</td>
<td>Specify the realm for this connection that is used when a user logs onto the endpoint. The connection ignores any other realm available for the user's login credentials.</td>
<td>Editable</td>
</tr>
<tr>
<td>Preferred User Role Set</td>
<td>Specify the preferred role or the name of the rule for the role set to be used for user authentication. The role or rule name used must be a member of the preferred user realm.</td>
<td>Editable</td>
</tr>
<tr>
<td>Select client certificate from machine certificate store</td>
<td>When this check box is selected, the Pulse connection looks at client certificates located in the Local Computer personal certificate store. When this check box is not selected, the connection accesses the user certificate store as a Windows endpoint.</td>
<td>Editable</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Editable/Non-Editable/Invalid</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Connections</td>
<td>Click New button to add a new connection.</td>
<td>Non-Editable</td>
</tr>
<tr>
<td></td>
<td>Click Delete button to delete an existing connection.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:**

There can be only one SDP enabled PDC connection at a time. Administrator cannot add a new connection or delete the existing SDP enabled PDC connection.

- Editable, - Non-Editable, - Invalid Settings

Figure 98: Connection Settings
Figure 99: Connection Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to override connection policy</td>
<td>✅</td>
</tr>
<tr>
<td>Lock down this connection</td>
<td>✗</td>
</tr>
<tr>
<td>Enable stealth mode on this connection</td>
<td>✗</td>
</tr>
<tr>
<td>Show stealth connection to users</td>
<td>✗</td>
</tr>
<tr>
<td>Support Remote Access (Connect Secure) or LAN Access (Policy Secure) on this connection</td>
<td>✗</td>
</tr>
<tr>
<td>Enable Pulse Collaboration integration on this connection</td>
<td>✗</td>
</tr>
<tr>
<td>Connect to URL of this server only</td>
<td>✅</td>
</tr>
<tr>
<td>List of Connection URLs</td>
<td></td>
</tr>
<tr>
<td>Attempt most recently connected URL, first</td>
<td>✅</td>
</tr>
<tr>
<td>Randomize URL list order</td>
<td>✅</td>
</tr>
<tr>
<td>Use Desktop Credentials</td>
<td>✅</td>
</tr>
</tbody>
</table>
Figure 100: Connection Settings
Troubleshooting

This section outlines common error messages or problems encountered during the onboarding or authentication to the SDP controller.

1. **Scenario** - User is onboarded and enrolled to the SDP controller. When the user selects the certificate while connecting to the SDP controller, user might get the following error message and the notification as shown in the screens below:

   **Figure 101: Certificate Error Message**

   ![Certificate Error Message](image)

   **Figure 102: Certificate Error Notification**

   ![Certificate Error Notification](image)

   **Possible Causes:**

   There might be one of the following reasons for the certification error:

   a. Certificate is expired.
      
      **Possible Solution:** Admin needs to check the validity of the certificate and renew the certificate.

   b. Certificate is invalid.
      
      **Possible Solution:** In AAA service, under **AAA service > Trusted Client CA**, verify that the CA certificate is present or not.

2. **Scenario** - When the user attempts to onboard, SDP enabled PDC onboarding gets failed.

   Now, when the user **sdpuser1** attempts to onboard, onboarding gets failed and the following error message gets displayed:
Figure 103: Onboarding Failed

Possible Cause: Pulse Workspace supports maximum five devices per user.

As shown in the following screen, Pulse Workspace has already five devices onboarded for the user (sdpuser1).

Figure 104: Pulse Workspace

Possible Solution: Administrator can delete any unwanted or unused device for the successful onboarding.

Possible Cause: Due to mismatch of the TLS versions on Pulse One and Windows 7.

Possible Solution: Install the following security update on Windows 7.


3. Scenario – The user clicks Disconnect button to disconnect the SDP enabled PDC connection and SDP enabled PDC connection details are disappeared. Refer to the screenshot below:
Figure 105: No Connections

Possible Cause:
On PWS, verify that the SDP enabled PDC connection exists or not. This connection might have got deleted from the PWS. Here the user is unaware about the deleted SDP enabled PDC connection in Pulse Workspace.

Possible Solution:
User might need to onboard again. Refer to the section SDP Enabled Pulse Desktop Client Onboarding.
Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, then file a ticket with PSGSC.

- Product warranties—For product warranty information, visit https://www.pulsesecure.net.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure, LLC has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.pulsesecure.net/support
- Search for known bugs: https://www.pulsesecure.net/support
- Find product documentation: https://www.pulsesecure.net/techpubs
- Find solutions and answer questions using our Knowledge Base: https://www.pulsesecure.net/support
- Download the latest versions of software and review release notes: https://www.pulsesecure.net/support
- Search technical bulletins for relevant hardware and software notifications: https://www.pulsesecure.net/support
- Open a case online in the CSC Case Management tool: https://www.pulsesecure.net/support

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://www.pulsesecure.net/support

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at https://www.pulsesecure.net/support
- Call 1-844-751-7629 (toll-free in the USA).

For international or direct-dial options in countries without toll-free numbers, see https://www.pulsesecure.net/support.
References

- Software Defined Perimeter Getting Started Guide
- Software Defined Perimeter Supported Platforms Guide
- Pulse One Administration Guide
- Pulse Workspace Administration Guide
- Pulse Connect Secure Administration Guide
- Pulse Desktop Client Administration Guide

Find product documentation: https://www.pulsesecure.net/techpubs