BeyondTrust

Password Safe Cloud
Resource Broker Install & Config Guide 21.1

TC:4/30/2021

Table of Contents

Password Safe Cloud Resource Broker Installation and Configuration Guide

This document explains how Password Safe Cloud uses resource brokers within resource zones to manage resources across segmented networks and how to configure resource zones.

A resource zone is a group of resources on your network. You can create an unlimited number of resource zones to meet the requirements for how your network is segmented; however, one zone for your entire network is sufficient. At least one resource zone is required. Password Safe Cloud creates a default resource zone called **Default**, which is a catch-all for all domains and workgroups in your network.

Password Safe Cloud uses resource brokers to communicate with the systems in your resource zones. A resource broker is a bundle of software that contains all of the services and components required for Password Safe Cloud to interact with your on-premises servers using TCP 443 for communication.

You must download the **Resource Broker Installer** from the Password Safe Cloud portal and install the broker on a Windows Server 2019 x64 or greater system in your network. Each resource zone must have at least one resource broker installed, but we recommend you install two or more for efficiency and redundancy of functionality. You may install up to ten resource brokers in each resource zone.

Note: *Installing a resource broker on Wiindows 2016 x64 is supported; however, Windows 2019 x64 is recommended.*

A resource zone uses a collection of resource brokers to handle the following four core Password Safe functions. Azure uses a round-robin technique to communicate with the resource brokers within the zone to handle these functions.

- **Authentication against LDAP/Active Directory**: Allows authentication into Password Safe against your local LDAP/Active Directory domains.
- **Asset and Account Discovery**: Uses a discovery scanning agent to discover assets and accounts in your network.
- **Credential Management**: Changes passwords or SSH keys on a scheduled or on-demand basis.
- **Session Proxy**: Acts as a proxy to allow a standard user to open SSH or RDP sessions on systems in your network.

For more information on the services that are bundled with a resource broker, please see Troubleshoot Resource Brokers Services .

Resource Broker Installation Prerequisites

Resource Broker requires software, hardware, and system resources as detailed below.

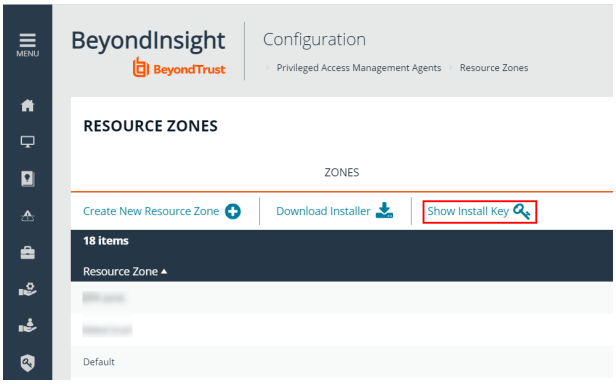
Component	Requirement
Operating System	Windows Server x64 2016 (minimum) Windows Server x64 2019 (recommended) ***Note:*** *Server Core edition is not supported.*
Processor	4 cores
Memory	16GB
Disk	100MB (for Resource Broker software) 64GB (for local caching of sessions) ***Note:*** *64GB allows for 14 days worth of sessions, assuming about 200 RDP and 200 SSH sessions per day, where the average session time is about one hour per session. RDP sessions would be 4.2GB per day; SSH sessions would be 0.3 GB per day.*
Server Requirements	Microsoft .NET Framework version 4.7.2 on Windows Server 2016 • Must be be preinstalled manually, or internet connectivity must be present to allow for dynamic installation. • For this method, **IE Enhanced Security** must be disabled from Server Manager. TLS 1.2 • If the Resource Broker installation is successful, then this is already enabled and no changes are needed. • If the installation is unsuccessful and exhibits the error described in the TLS Configuration section, then see the resolution provided there. ***Note:*** *If a web proxy is between the Resource Broker and Azure, the Resource Broker install will likely fail.*

Install a Resource Broker

Each resource zone must have at least one resource broker installed on a Windows 2019 x64 server in your network. If your deployment has only one resource zone, which is **Default**, you must install at least one resource broker in the **Default** zone. We recommend installing two or more resource brokers in each resource zone for work distribution and redundancy.

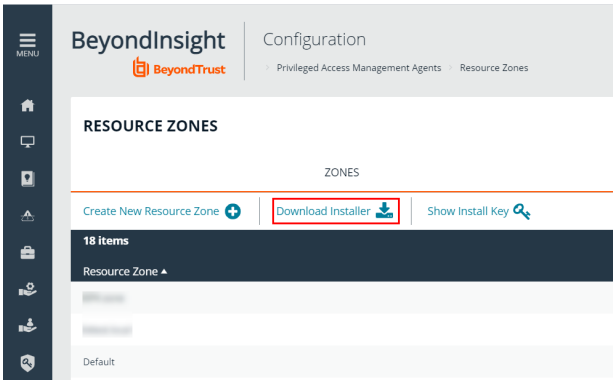
Download the Resource Broker Bundle and Install the Resource Broker

1. From the left menu in BeyondInsight, click **Configuration**.
2. Under **Privileged Access Management Agents**, click **Resource Zones**.
3. Click **Show Install Key**.



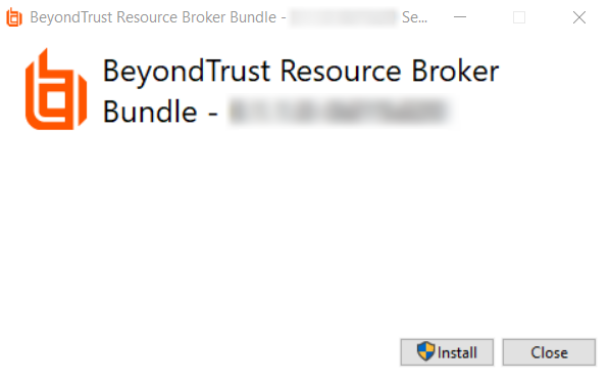
4. Click the **Copy** button to copy the installer key. The installer key is required for step 9.

5. Click **Download Installer**.

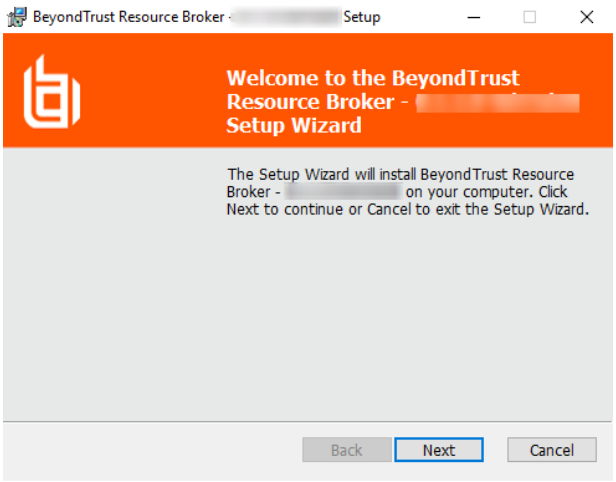


6. Copy the downloaded **BeyondTrust.Agents.Bootstrapper.exe** file to the Windows server where you would like to install the resource broker, and then run the file.

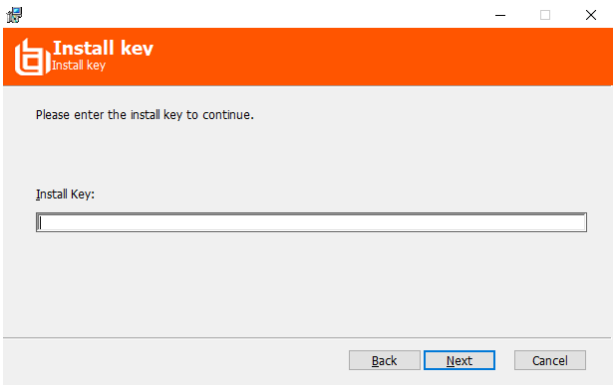
7. Click **Install**.



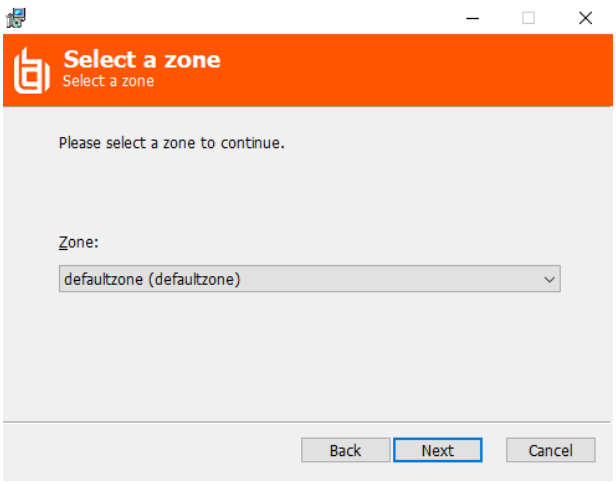
8. Click **Next** on the welcome screen.



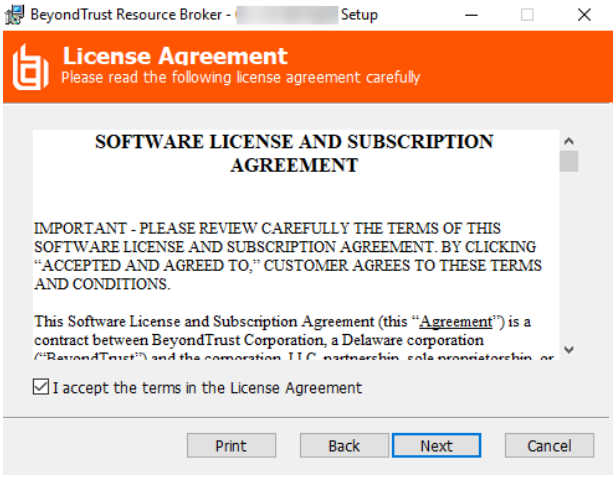
9. Paste the **Install Key** that you copied in step 3 into the **Install Key** field, and then click **Next**.



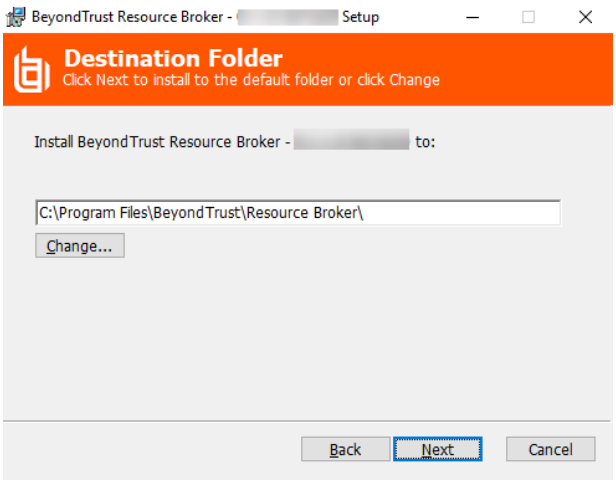
10. Select a resource zone from the **Zone** list, and then click **Next**.



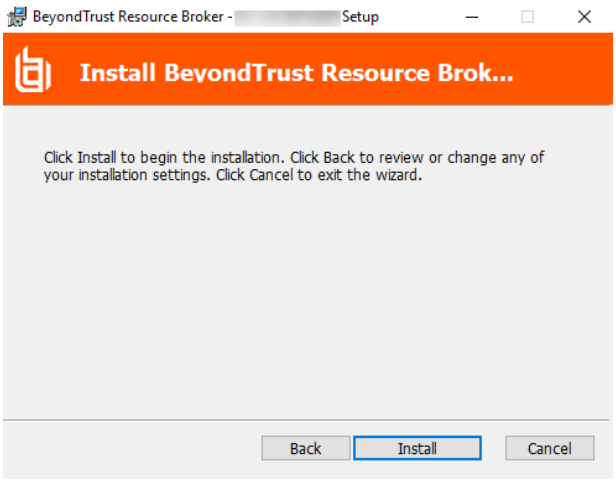
11. Check the box to accept the licence agreement terms, and then click **Next**.



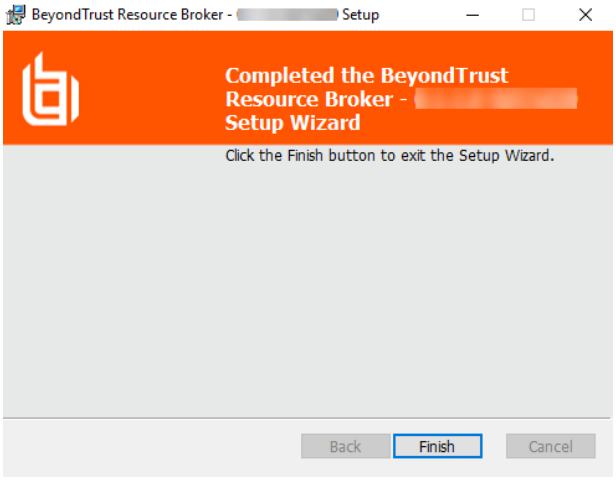
12. Click **Next** to install to the default folder or click **Change** to install to a different folder, and then click **Next**.



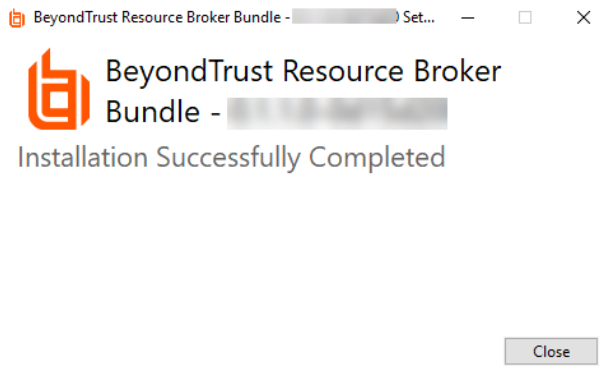
13. Click **Install** to begin the installation.



14. Click **Finish** to complete the Setup Wizard.



15. Click **Close** on the **Installation Successfully Completed** screen.



16. Go the BeyondInsight homepage to validate the dynamic dashboard has updated the **Resource Zones** and **Resource Brokers** tiles for this newly installed resource broker.

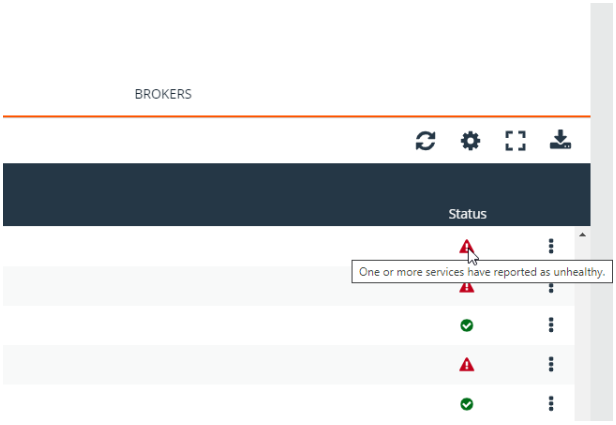
> ***Note:*** *Resource brokers automatically update as part of the Password Safe Cloud upgrade process. When the Password Safe console updates, deployed resource brokers automatically request an update and upgrade. If an error is*

encountered during the automatic upgrade process, an updated installer can be downloaded from the Password Safe console and installed manually, following the process above.

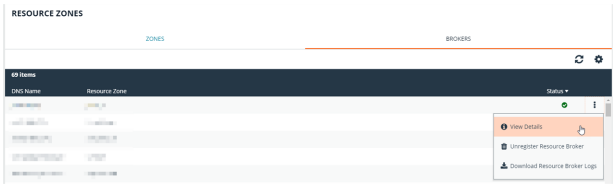
Manage Resource Brokers

From the **Brokers** grid on the **Resource Zones** page, you can check the health status for your resource brokers. Each of the services for a specific resource broker checks into PS Cloud independently with a heartbeat every 5 minutes. You can also unregister and delete resource brokers from this page.

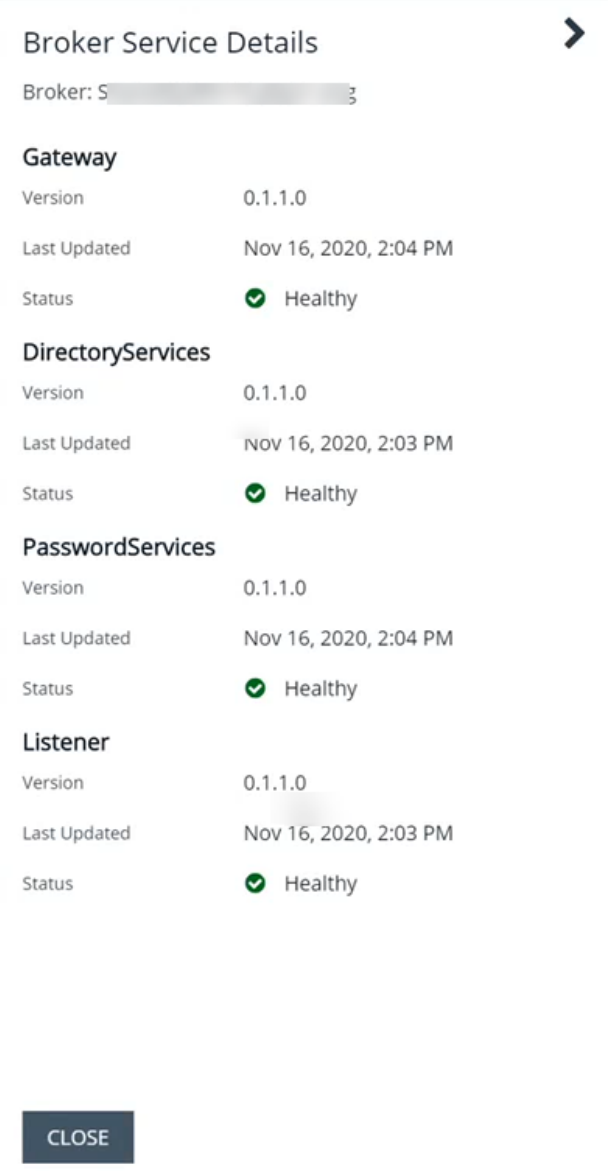
1. From the left menu in BeyondInsight, click **Configuration**.
2. Under **Privileged Access Management Agents**, click **Resource Zones**.
3. Click **Brokers**.
4. Look at the **Status** column for the resource broker to view its health status. A red warning symbol appears if one of the services misses two heartbeat intervals (hasn't checked in for 10 minutes). A green check mark displays if all of the services for that broker have checked in as healthy.



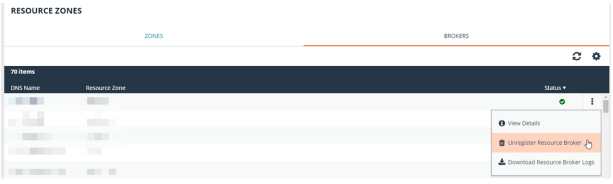
5. To view the details for the services on a specific broker, select the resource broker, click the **More Options** (vertical ellipsis) button, and then click **View Details**.



6. You can review the version, the time the service last updated, and the health status for each service on the broker.



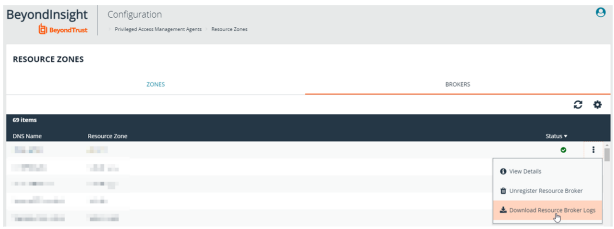
7. To delete a resource broker, you must manually uninstall it from the system where it was installed. This automatically unregisters the resource broker from the zone. To remove it from the **Resource Zones** page, click the **More Options** (vertical ellipsis) button for the broker, click **Unregister Resource Broker**, and then click **Delete** on the confirmation message that appears.



Download Resource Broker Logs

From the **Brokers** grid on the **Resource Zones** page, you can request and download resource broker log files.

1. From the left menu in BeyondInsight, click **Configuration**.
2. Under **Privileged Access Management Agents**, click **Resource Zones**.
3. Click **Brokers**.
4. For the resource broker logs, click the **More Options** (vertical ellipsis) button, and then select **Download Resource Broker Logs**.
5. A pop up message confirms the download is preparing, and the logs download to your device, as one compressed file.
6. Open the compressed file to view the log files available, and select the log file to view. Log files are in plain text (.txt) format.



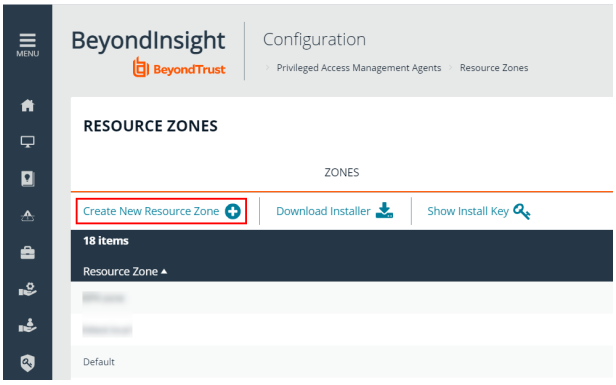
Configure Resource Zones

Create a Resource Zone

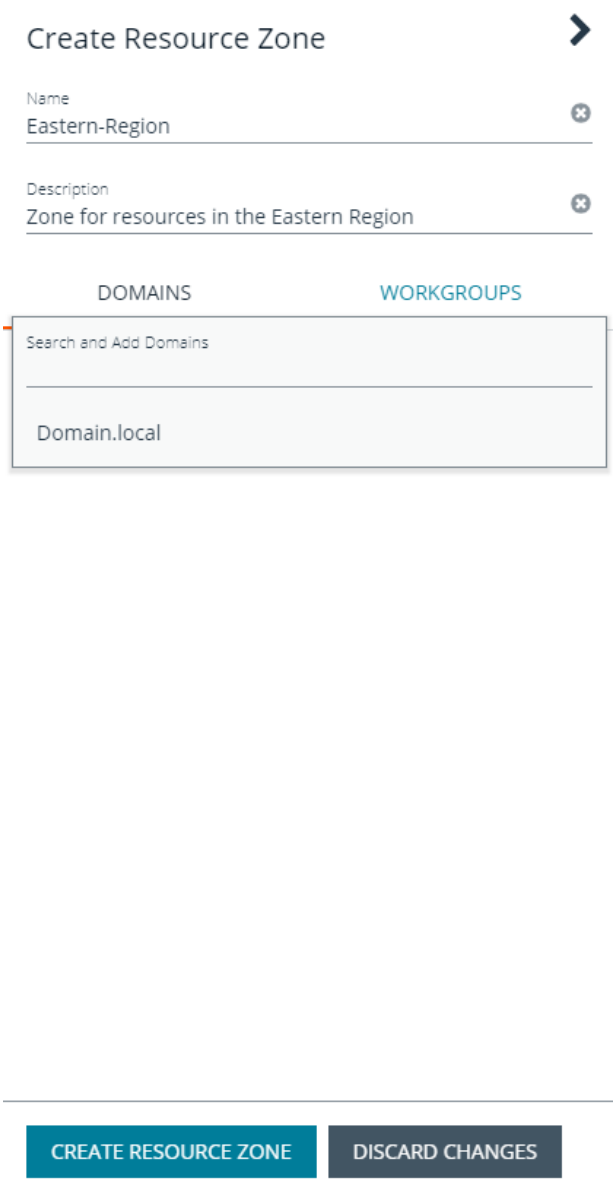
You may create as many resource zones as needed for your environment; however, only one resource zone is required. This is the built-in **Default** zone, which is a catch-all for all domains and workgroups in your network.

To create a new resource zone:

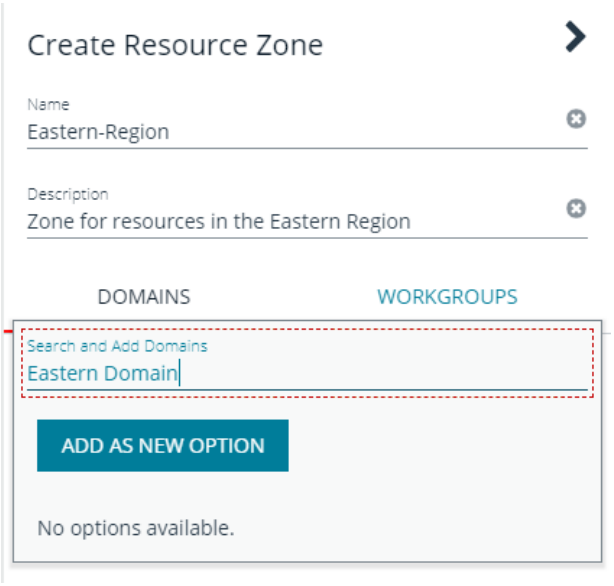
1. From the left menu in BeyondInsight, click **Configuration**.
2. Under **Privileged Access Management**, click **Resource Zones**.
3. Click **Create a New Resource Zone**.



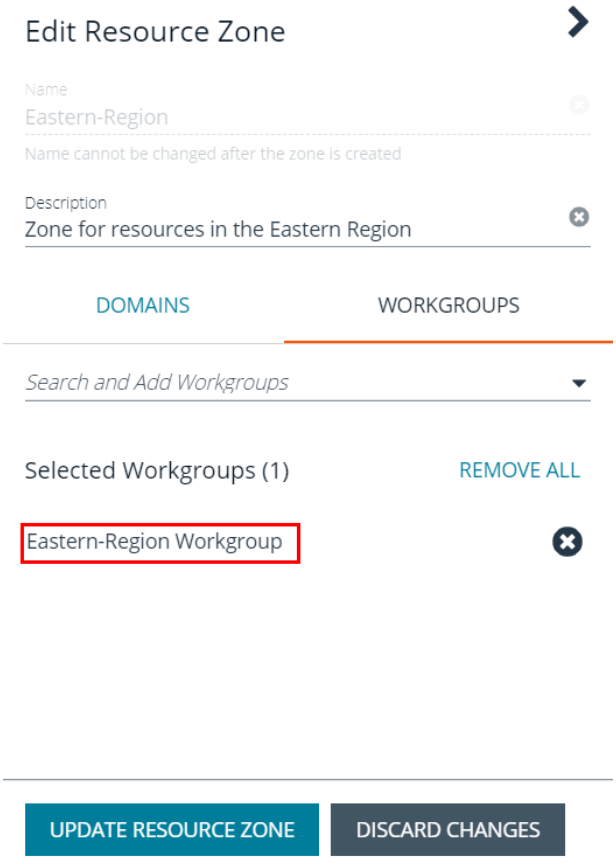
4. Enter a **Name** for identifying the resource zone. This can be up to 64 characters and cannot contain spaces.
5. Enter a meaningful **Description**.
6. Under **Domains**, select a domain from the list or enter a domain name or an LDAP server name, if it isn't listed.



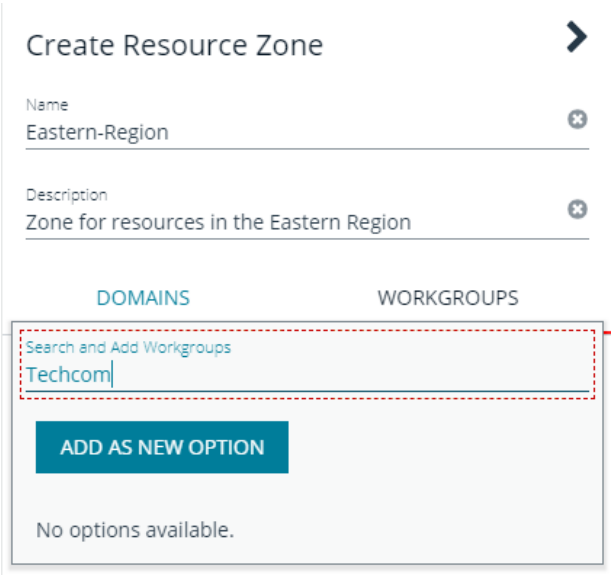
> ***Tip:*** *A domain or LDAP server is used for anything that Password Safe needs to obtain from a directory, such as authentication, directory queries, directory credentials, binding credentials, etc. Domains and LDAP servers that have already been discovered in Password Safe and are not already associated with a resource zone are listed. You can manually add a domain or LDAP server that has not yet been discovered by typing it in the* ***Search and Add Domains*** *box, and then clicking the* ***Add as New Option*** *button.*



7. For **Workgroups**, do not select or enter any. Instead, allow Password Safe to automatically create a workgroup using the name of the resource zone once the zone is created.



> ***Tip:*** *A workgroup is used to segment functionality within Password Safe Cloud to specific managed systems. Existing workgroups that are not already associated with a resource zone are listed. You can manually add a workgroup by typing it in the* ***Search and Add Workgroups*** *box, and then clicking the* ***Add as New Option*** *button.*



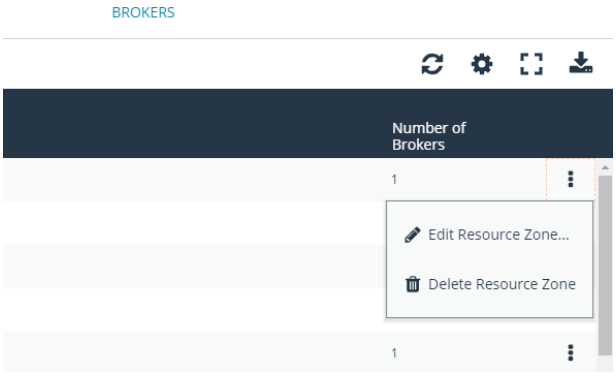
8. Click **Create Resource Zone**.

Edit and Delete Resource Zones

You can edit or delete resource zones as follows:

Select the resource zone in the grid on the **Resource Zones** page, click the **More Options** (ellipsis) button, and then select **Edit Resource Zone** or **Delete Resource Zone**.

> ***Note:*** *Editing a resource zone provides the same options as creating a resource zone, as documented in the steps above. You cannot delete a resource zone that has resource brokers associated with it. You must unregister all resource brokers from the zone first.*



Troubleshoot Resource Broker Issues

Error: "The client and server cannot communicate, because they do not possess a common algorithm"

Summary

When trying to install the Resource Broker Bundle, after entering the install key, you receive a communication error indicating "*The client and server cannot communicate, because they do not possess a common algorithm*". The following exception is indicated in the install log:

```
Failed to execute SetComboboxZonesCustomAction

System.AggregateException: One or more errors occurred. ---> System.Net.Http.HttpRequestException:
An error occurred while sending the request. ---> System.Net.WebException: The underlying connection
was closed: An unexpected error occurred on a receive. —> System.ComponentModel.Win32Exception: The
client and server cannot communicate, because they do not possess a common algorithm

at System.Net.SSPIWrapper.AcquireCredentialsHandle(SSPIInterface SecModule, String package,
CredentialUse intent, SecureCredential scc)
at System.Net.Security.SecureChannel.AcquireCredentialsHandle(CredentialUse credUsage,
SecureCredential& secureCredential)
at System.Net.Security.SecureChannel.AcquireClientCredentials(Byte[]& thumbPrint)
at System.Net.Security.SecureChannel.GenerateToken(Byte[] input, Int32 offset, Int32 count, Byte[]&
output)
at System.Net.Security.SecureChannel.NextMessage(Byte[] incoming, Int32 offset, Int32 count)
at System.Net.Security.SslState.StartSendBlob(Byte[] incoming, Int32 count, AsyncProtocolRequest
asyncRequest)
at System.Net.Security.SslState.ForceAuthentication(Boolean receiveFirst, Byte[] buffer,
AsyncProtocolRequest asyncRequest)
at System.Net.Security.SslState.ProcessAuthentication(LazyAsyncResult lazyResult)
at System.Threading.ExecutionContext.RunInternal(ExecutionContext executionContext, ContextCallback
callback, Object state, Boolean preserveSyncCtx)
at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback
callback, Object state, Boolean preserveSyncCtx)
at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback
callback, Object state)
at System.Net.TlsStream.ProcessAuthentication(LazyAsyncResult result)
at System.Net.TlsStream.Write(Byte[] buffer, Int32 offset, Int32 size)at
System.Net.ConnectStream.WriteHeaders(Boolean async)
```

Cause

If the .NET framework version is less than 4.6, the **SchUseStrongCrypto** registry key defaults to **0**. This key must have a value of **1** to use TLS 1.2. If .NET is greater than 4.6, this registry key defaults to **1** without having to make changes to it.

Resolution

Set the **SchUseStrongCrypto (DWORD)** registry key found under **HKLM\SOFTWARE\Microsoft\.NETFramework\v4.0.30319** to a value of **1** to force the use of TLS 1.2, and then restart the system.

> ***Note:*** *If the* ***SchUseStrongCrypto*** *registry key does not exist, you must create it.*

Resource Broker Service Details

A resource broker bundle installs the following services on the Windows server where you run the bootstrapped install file:

- Resource Broker Gateway
- Resource Broker Listener
- Password Services
- Directory Services
- Discovery Scanner
- Session Monitoring

We have outlined the details for each of these services below.

Resource Broker Gateway

- Service properties:
  - **Service name**: **bt_resourcebrokergateway_agent**
  - **Display name**: **BeyondTrust Resource Broker Gateway Agent**
- Acts as the local services communication hub for all zone and agent requests.
  - Proxies all requests down to the directory, password, and session monitoring services from the resource broker listening agent (described in next section)
  - Proxies all requests up to the Azure Relay Hybrid Connection in the PS Cloud instance
- Executes password tests and password changes for managed systems and managed accounts.
- Handles the initial resource broker registration and configuration.
- Contains platform-specific modules.
- Sends heartbeat to cloud every 5 minutes.
- Utilizes PS Cloud identity service as the API authority. All requests to this service receive a token from the PS Cloud identity service.
- Log files for this service are located in **C:\Program Files\BeyondTrust\Resource Broker\ResoureBrokerGateway\logs**.

> *For more information on Azure Relay Hybrid Connections, please see Azure Relay Hybrid Connections protocol at https://docs.microsoft.com/en-us/azure/azure-relay/relay-hybrid-connections-protocol.*

Resource Broker Listener

- Service properties:
  - **Service name**: **bt_resourcebrokerlistener_agent**
  - **Display name**: **BeyondTrust Resource Broker Agent**

- Acts as a reverse proxy for all requests from Password Safe Cloud for a resource zone through the Azure Relay Hybrid Connection in a round-robin process.
- Forwards requests to the Resource Broker Gateway.
- Listens on a zone-specific hybrid connection for resource-specific requests, such as password tests and directory queries.
- Listens on an agent-specific hybrid connection for target-specific requests, such as session monitoring.
- Sends heartbeat to cloud every 5 minutes
- Log files for this service are located in **C:\Program Files\BeyondTrust\Resource Broker\ResoureBrokerListener\logs**.

Password Services

- Service properties:
    - **Service name**: **bt_passwordservices_agent**
    - **Display name**: **BeyondTrust Password Services Agent**
- Executes password tests and password changes for managed systems and managed accounts.
- Contains platform specific modules.
- Sends heartbeat to cloud every 5 minutes.
- Utilizes PS Cloud identity service as the API authority. All requests to this service receive a token from the PS Cloud identity service.
- Log files for this service are located in **C:\Program Files\BeyondTrust\Resource Broker\PasswordServices\logs**.

Directory Services

- Service properties:
    - **Service name**: **bt_directoryservices_agent**
    - **Display name**: **BeyondTrust Directory Services Agent**
- Executes the following Active Directory or LDAP actions:
    - Directory queries
    - Directory credentials tests
    - Group enumeration
    - User and group management
    - Authentication
- Sends heartbeat to cloud every 5 minutes.
- Utilizes PS Cloud identity service as the API authority. All requests to this service receive a token from the PS Cloud identity service.
- Log files for this service are located in **C:\Program Files\BeyondTrust\Resource Broker\DirectoryServices\logs**.

Discovery Scanner

- Service properties:
    - **Service name**: **btdiscoverysvc**
    - **Display name**: **BeyondTrust Discovery Service**

- Schedules and executes discovery scans.
- Is auto-configured by obtaining the configuration via the Resource Broker Gateway.
- Communicates directly to PS Cloud via the client certificate that Event Services uses for Central Policy.
- Requests bearer token from PS Cloud identity service for its initial configuration.

Note: *The scanner obtains the configuration upon startup only. Once it begins using central policy, it doesn't need to continue requesting the configuration.*

- Log files for this service are located in **C:\Program Files\BeyondTrust\Discovery\logs**.

Session Monitoring

- Service properties:
  - **Service name**: **btPBPSSM**
  - **Display name**: **BeyondTrust Session Monitoring**
- Session monitoring proxy for SSH and RDP sessions.
- Sessions are proxied through the local agent.
- The session is associated with a broker that responds in a zone round robin.
- Active session monitoring (locking + termination) are proxied from PS Cloud to the resource broker.
- Session io logs are are written locally to the resource broker and when a session is complete, the io logs are copied to your customer storage account in Azure.
- Session replay in PS Cloud is done directly from your customer storage account in Azure.
- Sends heartbeat to cloud every 5 minutes.
- Log files for this service are located in **C:\Program Files\BeyondTrust\Resource Broker\Session Manager\logs**.