

Azure Private Link

Entrust CSP Vault for Cloud Keys Integration Guide

2026/11/06

Member of
Microsoft Intelligent
Security Association

Microsoft Security

© Entrust Corporation. All rights reserved.

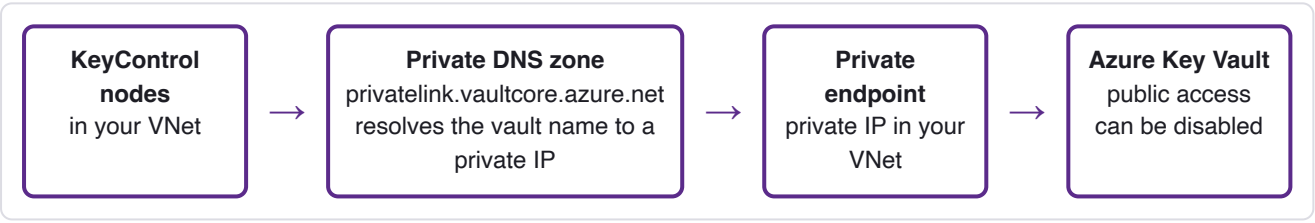
Using Azure Private Link with CSP Vault for Cloud Keys

Connect your KeyControl nodes to Azure Key Vault over a private network address (BYOK)

1. Overview

Azure Private Link gives your Azure Key Vault a private IP address inside your own virtual network (VNet). When the KeyControl nodes run in that VNet, or in a network that can resolve and reach it, CloudKeys operations reach the Key Vault without using its public address, and you can turn off public network access on the Key Vault.

No change to KeyControl is required. The setup is done in Azure: a private endpoint, a private DNS zone and a DNS link. The KeyControl nodes keep using the normal Key Vault name, for example `myvault.vault.azure.net`, which now resolves to the private address.



Tested by Entrust	Not tested by Entrust
KeyControl 10.6.1, two-node cluster in an Azure VNet; Azure Key Vault (Standard) and Azure Managed HSM (Standard) with a private endpoint; public network access disabled; create, rotate, disable, enable and delete CloudKeys (Key Vault: both nodes; Managed HSM: create, rotate, disable and enable from one node).	NOT TESTED Premium (HSM-backed) Key Vault keys, VPN, ExpressRoute, hub-and-spoke or on-premises DNS forwarding, outbound proxy, firewall rules.

2. Before you start

- KeyControl 10.6.1 nodes running in an Azure VNet (see *Deploying a CSP Vault Node in Azure* in the Administration Guide).
- An Azure Key Vault and an Azure service principal that KeyControl uses (Azure CSP account). The service principal needs Reader on the subscription (KeyControl lists vaults) and key permissions on the

Key Vault.

- Azure rights to create a private endpoint and a private DNS zone in the resource group.
- The Azure CLI (`az`) or the Azure portal. The steps below use the CLI.

3. Configure Azure

Step 1 - Create a subnet for private endpoints (if you do not have one)

```
az network vnet subnet create -g MYRG --vnet-name MYVNET -n snet-pe --address-prefixes MY-
SUBNET-PREFIX
```

Step 2 - Create the private DNS zone and link it to the VNet of every KeyControl node

```
az network private-dns zone create -g MYRG -n privatelink.vaultcore.azure.net
az network private-dns link vnet create -g MYRG -z privatelink.vaultcore.azure.net \
   -n kcv-link -v MYVNET -e false
```

> **Important:** the zone must be linked to the VNet where the KeyControl nodes run. Without the link the Key Vault name resolves to the public address and the operations fail (see Troubleshooting).

Step 3 - Create the private endpoint with its DNS registration

```
KVID=$(az keyvault show -g MYRG -n MYVAULT --query id -o tsv)
az network private-endpoint create -g MYRG -n pe-myvault --vnet-name MYVNET --subnet snet-pe \
   --private-connection-resource-id "$KVID" --group-id vault --connection-name myvault-conn
az network private-endpoint dns-zone-group create -g MYRG --endpoint-name pe-myvault -n myvault-
zg \
   --private-dns-zone privatelink.vaultcore.azure.net --zone-name vault
```

Check that the DNS zone now has an A record named after the vault:

```
az network private-dns record-set a list -g MYRG -z privatelink.vaultcore.azure.net -o table
```

Step 4 - Allow the service principal to use the Key Vault

Give the service principal key permissions on the Key Vault (access policy, or the Key Vault Crypto Officer role if the vault uses Azure RBAC).

Step 5 (optional) - Turn off public access

```
az keyvault update -g MYRG -n MYVAULT --public-network-access Disabled
```

> Do this only after step 6 works. Machines outside the VNet can no longer reach the vault, including the Azure CLI on your workstation.

4. Configure KeyControl

No Private Link specific setting exists in KeyControl. Use the normal CloudKeys procedure:

1. In the CloudKeys vault, open **CSP Accounts**, choose **Actions > Add CSP Account**, type **AZURE**, and enter the tenant, subscription, client and object IDs and the client secret.
2. Open **Key Sets**, choose **Actions > Create Key Set** and select the Azure CSP account.

3. Open **CloudKeys**, select the key set, type **Key Vault** and choose **Actions > Create CloudKey**. Choose your Key Vault in the list. The list is read from Azure and shows every Key Vault the service principal can read, including vaults that have no keys yet. No import is needed.
4. Optional: to bring keys that already exist in the Key Vault under KeyControl management, choose **Actions > Import CloudKeys**, type **Key Vault**, and select the vault.

5. Verify the private connection

1. With public network access disabled (step 5), create a CloudKey from KeyControl. It must succeed and show the status AVAILABLE.
2. From a machine outside the VNet, `az keyvault key list --vault-name MYVAULT` must fail with "Public network access is disabled and request is not from a trusted service nor via an approved private link". This shows that only the private path works.
3. Optional: enable Key Vault diagnostic logs and check that the caller address of the KeyControl requests is a private address from your VNet.

6. Troubleshooting

Symptom	Cause and fix
CloudKey operations fail with "Insufficient keyvault permissions ... Please review the permissions for the service principal" although the permissions did not change	In this situation the message can be misleading. The Key Vault may be refusing the connection because public access is disabled and the KeyControl node resolves the vault name to the public address. Check, in this order: (1) the private DNS zone is linked to the VNet of **every** KeyControl node; (2) the zone has an A record for the vault and the private endpoint connection is Approved; (3) a custom DNS server forwards `privatelink.vaultcore.azure.net` (or the vault name) to the Azure-provided DNS resolver; (4) only then review the service principal permissions.
A Key Vault is missing from the Key Vault list (key set details, or the Create CloudKey dialog)	The list is read from Azure and can take several seconds to appear; wait and refresh. If the vault is still missing, the service principal cannot see it in Azure: check that the vault is in the subscription of the CSP account and that the service principal has at least Reader on it (or on the subscription).
Name resolution result unclear	From a machine in the VNet, `nslookup myvault.vault.azure.net` must return the private address from the private endpoint subnet.

7. Other network designs

Design	Status
KeyControl nodes in an Azure VNet (this guide)	Tested
KeyControl on premises, connected through Site-to-Site VPN or ExpressRoute	`NOT TESTED` In principle the on-premises DNS must forward `vault.azure.net` and the privatelink zone to a resolver inside Azure (for example Azure DNS Private Resolver), and the on-premises network needs a route to the private endpoint subnet.

Hub-and-spoke VNets, VNet peering	`NOT TESTED` Link the private DNS zone to each VNet that contains KeyControl nodes.
Azure Managed HSM	Tested. Use group id `managedhsm` and the zone `privatelink.managedhsm.azure.net`. To disable public access, Azure requires both `--public-network-access Disabled` and `--default-action Deny` (`az keyvault update-hsm`). In KeyControl choose type **Managed HSM** when you create the CloudKey and leave **EKM Key** off (EKM is a different feature and was not tested).
Outbound firewall or proxy	`NOT TESTED` Allow Microsoft Entra ID and Azure Resource Manager; they are not covered by Private Link.

8. Notes

- Private Link has Azure costs (private endpoint per hour and data processed, private DNS zone). See Azure pricing.
- Do not enable purge protection on a vault if you want to permanently remove deleted keys during testing.
- The key dropdowns in KeyControl list every Key Vault the service principal can see. Use a service principal that has access to your own vaults only.

Entrust and Cryptographic Security Platform are trademarks of Entrust Corporation. Microsoft, Azure and Entra are trademarks of Microsoft.