Remote Support
Security Provider Integration:
Kerberos Configuration
# Table of Contents

Configure the Secure Remote Access Appliance for Kerberos Authentication .......... 3

Prerequisites ........................................................................................................... 3

Kerberos Security Provider Settings ................................................................. 3

SPN Use in BeyondTrust Software ................................................................. 4

Network Setup Examples ...................................................................................... 5

Network Setup Example 1: Kerberos KDC ......................................................... 5

Network Setup Example 2: Kerberos KDC and LDAP Server on the Same Network .... 7

Network Setup Example 3: Kerberos KDC and LDAP Server on Separate Networks ..10

Network Setup Example 4: Kerberos KDC in Multiple Realms .............................. 13
Configure the Secure Remote Access Appliance for Kerberos Authentication

BeyondTrust supports single sign-on functionality using the Kerberos authentication protocol, enabling users to authenticate to their BeyondTrust user accounts without having to enter credentials. This document details methods for integrating the Secure Remote Access Appliance in some typical Kerberos networking configurations. This document is intended to be used by trained individuals with a working knowledge of Kerberos. It is assumed that you either have an existing implementation of Kerberos deployed or are in the process of deploying a Kerberos implementation. As there are many possible Kerberos configuration implementations, this document serves only as a guide for standard implementations.

Prerequisites

Prior to integrating the Secure Remote Access Appliance with your Kerberos configuration, ensure the following requirements are met:

- You must have a working Kerberos Key Distribution Center (KDC).
- Clocks must be synchronized across all clients, the KDC, and the Secure Remote Access Appliance. Using a Network Time Protocol (NTP) is the recommended method of synchronization.
- You must have a service principal created on the KDC for your Secure Remote Access Appliance.

Kerberos Security Provider Settings

The most appropriate configuration for your Kerberos security provider depends on your overall authentication and network infrastructure, as well as where your Secure Remote Access Appliance is located in your network. The examples in the following section demonstrate typical setups, while the chart below explains each of the Kerberos security provider options.

| Keep display name synchronized with remote system | If selected, a Kerberos-authenticated user's display name will be their User Principal Name. If deselected, display names can be edited locally on the Secure Remote Access Appliance. |
| User Handling Mode | Allow all users | Allows anyone who currently authenticates via your KDC to log into your Secure Remote Access Appliance. |
| | Allow only user principals specified in the list | Allows only specified user principals to log into your Secure Remote Access Appliance. |
| | Allow only user principals that match the regex | Allows only user principals who match a Perl-compatible regular expression (PCRE) to log into your Secure Remote Access Appliance. |
| SPN Handling Mode | Allow all SPNs | Allow all configured Service Principal Names (SPNs) for this security provider. |
| | Allow only SPNs specified in the list | Allow only specific SPNs selected from a list of currently configured SPNs. |
| Default Policy | Select a group policy as the default for users authenticating against this Kerberos security provider. |
Browsers may use different methods to canonicalize the hostname for a site, including performing a reverse lookup of the IP of the hostname specified in the URL. The SPN canonicalization of this address may cause the browser to request an SPN based on an internal hostname rather than the appliance hostname.

For example, a BeyondTrust site built as hostname `support.example.com` may ultimately resolve to the hostname `internal.example.com`.

```
support.example.com → 10.0.0.1 → 1.0.0.10.in-addr.arpa → internal.example.com
```

The BeyondTrust software expects the SPN in the form of `HTTP/` followed by the hostname configured in the BeyondTrust software during purchases or upgrade (`HTTP/support.example.com`). If the browser canonicalizes the hostname to an internal hostname and uses that hostname for the SPN (`HTTP/internal.example.com`), authentication will fail unless you have registered SPNs for both `HTTP/internal.example.com` and `HTTP/support.example.com`, and installed them on your Secure Remote Access Appliance.

If SPNs for multiple hostnames are imported, the BeyondTrust software will use the site hostname to which it was previously able to connect as a client. Therefore, if you are experiencing Kerberos authentication issues, it is advised to import a keytab for each hostname to which the site might canonicalize.
Network Setup Examples

Network Setup Example 1: Kerberos KDC

For this example:

- The Secure Remote Access Appliance may or may not be located behind a corporate firewall.
- Representatives may or may not be on the same network as the Secure Remote Access Appliance.
- Representatives belong as members to a Kerberos realm.
- Representatives can communicate with their KDC (typically over port 88 UDP).

Konfiguration

1. On the Kerberos KDC, register an SPN for your Secure Remote Access Appliance hostname and then export the keytab for this SPN from your KDC.
2. Log into your Secure Remote Access Appliance’s /login interface.
4. Under Import Keytab, click Choose File, and then select the exported keytab to upload. You should now see this SPN under the list of Configured Principals.
5. Go to Users & Security > Security Providers. Click Add. From the dropdown, select Kerberos.

6. Create a unique name to help identify this provider.
7. Be sure to check the Enabled box.
8. Choose if you want to synchronize display names.
9. Optionally, select to remove the REALM portion from the User Principal Name when constructing the BeyondTrust username.
10. For User Handling Mode, select Allow all users.
11. For SPN Handling Mode, leave the box unchecked in order to allow all SPNs.
12. You may also select a default group policy for users who authenticate against this Kerberos server.
13. Click Save to save this security provider configuration.
Network Setup Example 2: Kerberos KDC and LDAP Server on the Same Network

For this example:

- The Secure Remote Access Appliance may or may not be located behind a corporate firewall.
- Representatives may or may not be on the same network as the Secure Remote Access Appliance.
- Representatives belong as members to a Kerberos realm.
- Representatives can communicate with their KDC (typically over port 88 UDP).
- An LDAP server exists (which may or may not be the same machine as the KDC) that maps user principal names to groups to which the users may belong.
- The Secure Remote Access Appliance can directly communicate with the LDAP server.

Configuration

1. On the Kerberos KDC, register an SPN for your Secure Remote Access Appliance hostname and then export the keytab for this SPN from your KDC.
2. Log into your Secure Remote Access Appliance’s /login interface.
3. Go to **Users & Security > Security Providers**. Click **Add**. From the dropdown, select **LDAP**.

4. Create a unique name to help identify this provider.
5. Be sure to check the **Enabled** box.
6. Choose if you want to synchronize display names.
7. For **Lookup Groups**, select either **Only perform group lookups** or **Allow user authentication and perform group lookups**.
8. Continue to configure the settings for this LDAP server.
9. For the **User Query**, enter a query that can tie the **User Principal Name** as supplied in the user’s Kerberos ticket to a single entry within your LDAP directory store.
10. Click **Save** to save this security provider configuration.
11. Go to **Users & Security > Kerberos Keytab**.
12. Under **Import Keytab**, click **Choose File**, and then select the exported keytab to upload. You should now see this SPN under the list of **Configured Principals**.

13. Go to **Users & Security > Security Providers**. Click **Add**. From the dropdown, select **Kerberos**.

14. Create a unique name to help identify this provider.
15. Be sure to check the **Enabled** box.
16. Choose if you want to synchronize display names.
17. Optionally, select to remove the REALM portion from the User Principal Name when constructing the BeyondTrust username.
18. For **User Handling Mode**, select **Allow all users**.
19. For **SPN Handling Mode**, leave the box unchecked in order to allow all SPNs.
20. In LDAP Group Lookup, select the server configured in this process and add it to the **Group Providers In Use** list.

21. You may also select a default group policy for users who authenticate against this Kerberos server.

22. Click **Save** to save this security provider configuration.

Network Setup Example 3: Kerberos KDC and LDAP Server on Separate Networks

For this example:

- The Secure Remote Access Appliance may or may not be located behind a corporate firewall.
- Representatives may or may not be on the same network as the Secure Remote Access Appliance.
- Representatives belong as members to a Kerberos realm.
- Representatives can communicate with their KDC (typically over port 88 UDP).
- An LDAP server exists (which may or may not be the same machine as the KDC) that maps user principal names to groups to which the users may belong.
- The Secure Remote Access Appliance cannot directly communicate with the LDAP server.

Configuration

1. On the Kerberos KDC, register an SPN for your Secure Remote Access Appliance hostname and then export the keytab for this SPN from your KDC.
2. Log into your Secure Remote Access Appliance’s /login interface.
3. Go to Users & Security > Security Providers. Click Add. From the dropdown, select LDAP.

4. Create a unique name to help identify this provider.
5. Be sure to check the Enabled box.
6. Choose if you want to synchronize display names.
7. For Lookup Groups, select either Only perform group lookups or Allow user authentication and perform group lookups.
8. Continue to configure the settings for this LDAP server.
9. Because the LDAP server does not have direct communication with the Secure Remote Access Appliance, check the option Proxy from appliance through the Connection Agent.
10. Create a password for the connection agent.
11. Click Download Connection Agent to install the agent on a system behind your firewall. When installing the connection agent, provide the name and password you created for this LDAP server.
12. For the User Query, enter a query that can tie the User Principal Name as supplied in the user's Kerberos ticket to a single entry within your LDAP directory store.
13. Click Save to save this security provider configuration.
15. Under Import Keytab, click Choose File, and then select the exported keytab to upload. You should now see this SPN under the list of Configured Principals.

17. Create a unique name to help identify this provider.
18. Be sure to check the Enabled box.
19. Choose if you want to synchronize display names.
20. Optionally, select to remove the REALM portion from the User Principal Name when constructing the BeyondTrust username.
21. For User Handling Mode, select Allow all users.
22. For SPN Handling Mode, leave the box unchecked in order to allow all SPNs.
23. In LDAP Group Lookup, select the server configured in this process and add it to the Group Providers In Use list.
24. You may also select a default group policy for users who authenticate against this Kerberos server.
25. Click Save to save this security provider configuration.

Network Setup Example 4: Kerberos KDC in Multiple Realms

For this example:

- The Secure Remote Access Appliance may or may not be located behind a corporate firewall.
- Representatives may or may not be on the same network as the Secure Remote Access Appliance.
- Representatives may belong as members of multiple Kerberos realms existing in the corporate infrastructure (traditionally, a multi-domain hierarchy in Windows).
- If a DMZ realm exists, the representatives’ realms may have inbound trusts with that DMZ realm, allowing principals in the trusted realms to obtain tickets for services in the DMZ realm.

**Configuration**

1. Register one or more of the SPNs according to the following rules:
   - If a DMZ Kerberos realm is involved, register a unique SPN within the DMZ realm.
   - If no DMZ Kerberos realm is involved and no trust exists between the two realms, register a unique SPN in each realm.
   - If no DMZ Kerberos realm is involved and trust exists between the two realms, register a unique SPN in a realm of your choosing.

2. Export all registered SPNs.

4. Go to **Users & Security > Kerberos Keytab**.

5. Under **Import Keytab**, click **Choose File**, and then select the exported keytab to upload. You should now see this SPN under the list of **Configured Principals**.

6. Repeat the previous step for each exported keytab.

7. Go to **Users & Security > Security Providers**. Click **Add**. From the dropdown, select **Kerberos**.

8. Create a unique name to help identify this provider.

9. Be sure to check the **Enabled** box.

10. Choose if you want to synchronize display names.

11. Optionally, select to remove the REALM portion from the User Principal Name when constructing the BeyondTrust username.

12. If using a DMZ realm or using the same SPN for multiple realms, you will want to match on user principle name to identify users from the first realm.

13. If you registered multiple SPNs, choose the SPN that users from the first realm will use.

14. You may also select a default group policy for users who authenticate against this Kerberos server.

15. Click **Save** to save this security provider configuration.

16. Repeat steps 7 through 15 for each realm from which users will authenticate, substituting the UPN or SPN rule for each realm as appropriate.