BeyondTrust

Remote Support
Security Provider Integration:
Kerberos Server

TC:2/8/2019

Table of Contents

Kerberos Server for Single Sign-On

Integration of your BeyondTrust Appliance with external security providers enables administrators to efficiently manage user access to BeyondTrust accounts by authenticating users against external directory stores. This guide is designed to help you configure the BeyondTrust Appliance to communicate with a Kerberos security provider for the purpose of user authentication.

> ***Note:*** *To define group policies based upon groups within a remote server, you must configure both the LDAP group provider and the Kerberos user provider. You then must enable group lookup from the user provider's configuration page. One group security provider can be used to authorize users from multiple servers, including LDAP, RADIUS, and Kerberos. For group policy setup and for other security provider configurations, see the additional guides provided at www.beyondtrust.com/docs.*

Should you need any assistance, please contact BeyondTrust Technical Support at help.bomgar.com.

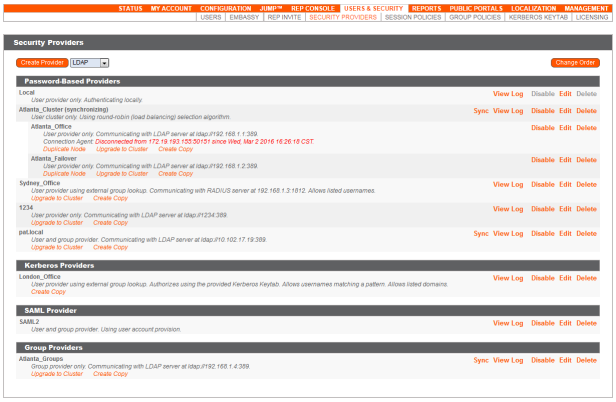
Create and Configure the Kerberos Security Provider

Go to **/login > Users & Security > Security Providers**.

From the dropdown, select the type of server you want to configure. Then click the **Create Provider** button.

Alternatively, you can copy an existing provider configuration by clicking **Create Copy**.

Enter the settings for this security provider configuration as detailed below.



General Settings

Name

Create a unique name to help identify this provider.

Enabled: This provider is enabled

If checked, your BeyondTrust Appliance can search this security provider when a user attempts to log in. If unchecked, this provider will not be searched.

User and Display Names: Keep display name synchronized with remote system

These values determine which fields should be used as the user's private and public display names.

Strip realm from principal names

Select this option to remove the REALM portion from the User Principal Name when constructing the BeyondTrust username.

Authorization Settings

User Handling Mode

Select which users can authenticate to your BeyondTrust Appliance. **Allow all users** allows anyone who currently authenticates via your KDC. **Allow only user principals specified in the list** allows only user principles explicitly designated. **Allow only user principals that match the regex** allows only users principals who match a Perl-compatible regular expression (PCRE).

SPN Handling Mode: Allow only SPNs specified in the list

If unchecked, all configured Service Principal Names (SPNs) for this security provider are allowed. If checked, select specific SPNs from a list of currently configured SPNs.

LDAP Group Lookup

If you want users on this security provider to be associated with their groups on a separate LDAP server, choose one or more LDAP group servers to use for group lookup.

Default Group Policy

Each user who authenticates against an external server must be a member of at least one group policy in order to authenticate to your BeyondTrust Appliance, logging into either the /login interface or the representative console. You can select a default group policy to apply to all users allowed to authenticate against the configured server.

Note that if a default policy is defined, then any allowed user who authenticates against this server will potentially have access at the level of this default policy. Therefore, it is recommended that you set the default to a policy with minimum privileges to prevent users from gaining permissions that you do not wish them to have.

Note: *If a user is in a default group policy and is then specifically added to another group policy, the settings for the specific policy will always take precedence over the settings for the default, even if the specific policy is a lower priority than the default, and even if the default policy's settings are set to disallow override.*

Save Changes

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

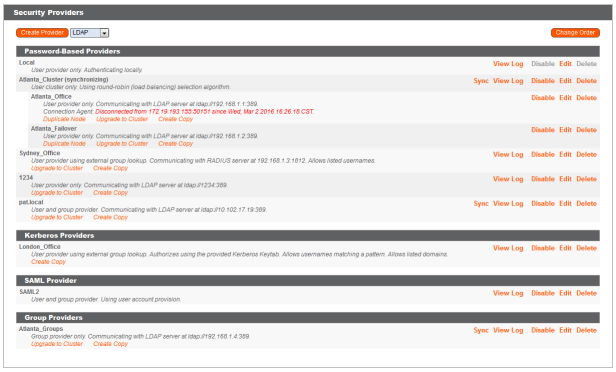
Prioritize and Manage Security Providers: Kerberos Servers

Change Order

Once you have set up your security providers, you can configure the order in which your BeyondTrust Appliance attempts to authenticate users.

On the **Security Providers** page, click **Change Order**. Then drag and drop the configured providers to set their priority. Clustered servers move as one unit and can be prioritized within the cluster.

After making changes to the order of priority, click the **Save Changes** button.



Sync

Synchronize the users and groups associated with an external security provider. Synchronization occurs automatically once a day. Clicking this button forces a manual synchronization.

View Log

View the status history for a security provider connection.

Disable

Disable this security provider connection. This is useful for scheduled maintenance, when you want a server to be offline but not deleted.

Troubleshoot Kerberos Server Integration Errors

Failed Logins

If a user cannot log into BeyondTrust using valid credentials, please check that at least one of the following sets of criteria is met.

1. The user has been expressly added to an existing group policy.
2. A default group policy has been set for the security provider configuration created to access the server against which the user is authenticating.
3. The user is a member of a group that has been expressly added to an existing group policy, and both user authentication and group lookup are configured and linked.

Error 6ca and Slow Logins

1. A **6ca** error is a default response signifying that the BeyondTrust Appliance has not heard back from the DNS server. It may occur when attempting to log into the representative console.
2. If users are experiencing extremely slow logins or are receiving the **6ca** error, verify that DNS is configured in your /appliance interface.

Troubleshooting Individual Providers

When configuring an authentication method tied to group lookup, it is important to configure first user authentication, then group lookup, and finally group policy memberships. When troubleshooting, you will want to work in reverse.

1. Verify that the group policy is looking up valid data for a given provider and that you do not have any **@@@** characters in the **Policy Members** field.
2. Next, if a group provider is configured, verify that its connection settings are valid and that its group **Search Base DN** is in the proper format.
3. If you want to use group lookup, verify that the security provider is set to look up group memberships of authenticated users.
4. To test the user provider, set a default policy and see if your users are able to log in.