Remote Support

Security Provider Integration: RADIUS Server

Table of Contents

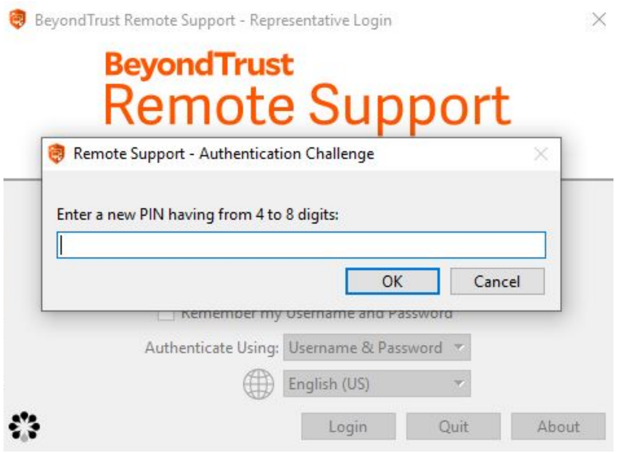
RADIUS Server for Authentication

Integration of your B Series 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 B Series Appliance to communicate with a RADIUS 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 RADIUS 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, please see the additional guides provided at https://www.beyondtrust.com/docs/remote-support/index.htm.*

Authenticate Using One-Time Passwords (OTP)

When using the Radius security provider, you can choose to use a one-time password (OTP) service provider, such as RSA SecurID. An OTP is simply a randomized password that is generated by a third-party service provider through a token or some other means and changes within a certain time frame to provide an extra layer of security upon login.



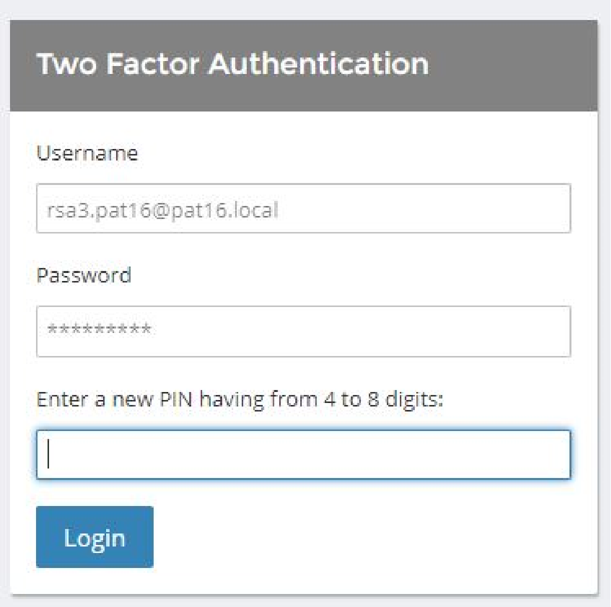
BeyondTrust Remote Support - Representative Login

Remote Support - Authentication Challenge

Enter a new PIN having from 4 to 8 digits:

Authenticate Using: Username & Password

Within your OTP provider's interface, you can configure a prompt to appear asking for credentials on the login screens for the BeyondTrust representative console and /login administrative interface. Once configured, users must enter their BeyondTrust username and password and then the OTP into the prompt.



Two Factor Authentication

Username

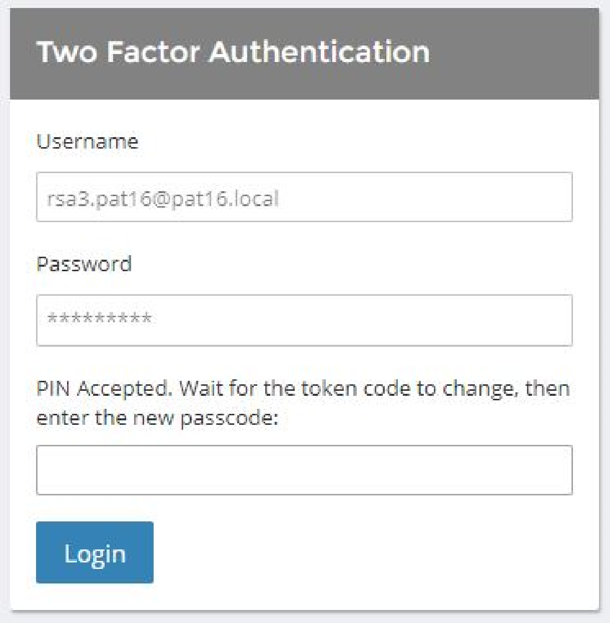
rsa3.pat16@pat16.local

Password

****

Enter a new PIN having from 4 to 8 digits:

If the OTP is entered correctly, access to the BeyondTrust representative console or /login administrative interface will be granted.



Two Factor Authentication

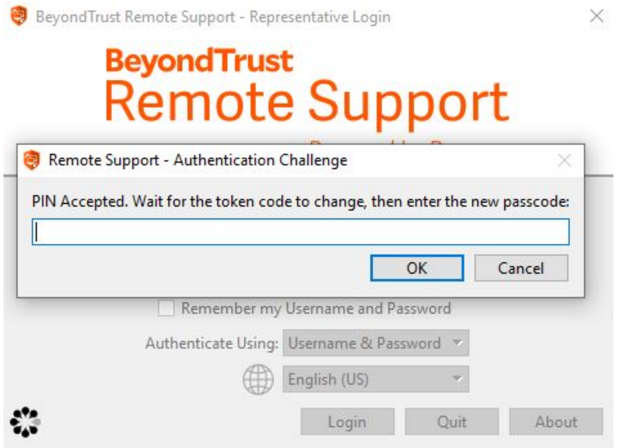
Username

rsa3.pat16@pat16.local

Password

****

PIN Accepted. Wait for the token code to change, then enter the new passcode:



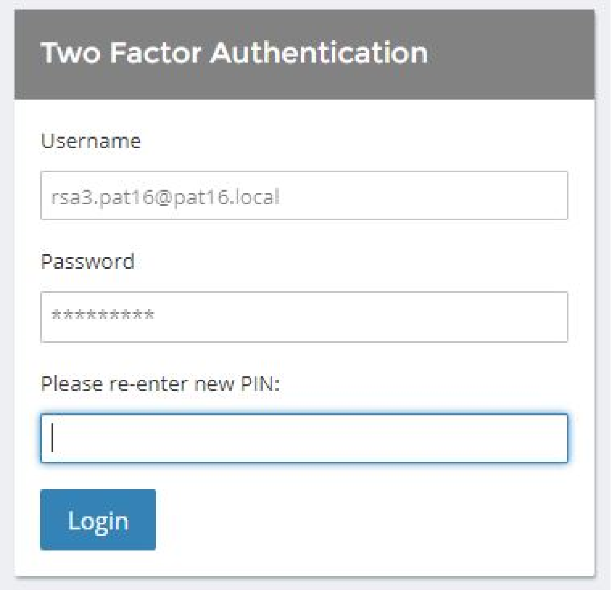
BeyondTrust Remote Support - Representative Login

Remote Support - Authentication Challenge

PIN Accepted. Wait for the token code to change, then enter the new passcode:

However, if the OTP is entered incorrectly, a new prompt will appear asking for the password to be re-entered.

Should you need any assistance, please log into the Customer Portal at https://beyondtrustcorp.service-now.com/csm to chat with Support.

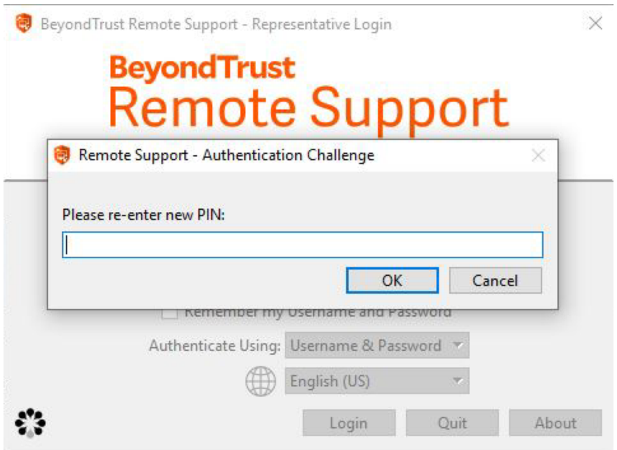


Two Factor Authentication

Username: rsa3.pat16@pat16.local

Password: *********

Please re-enter new PIN:



BeyondTrust Remote Support - Representative Login

BeyondTrust Remote Support

Remote Support - Authentication Challenge

Please re-enter new PIN:

□ Remember my Username and Password

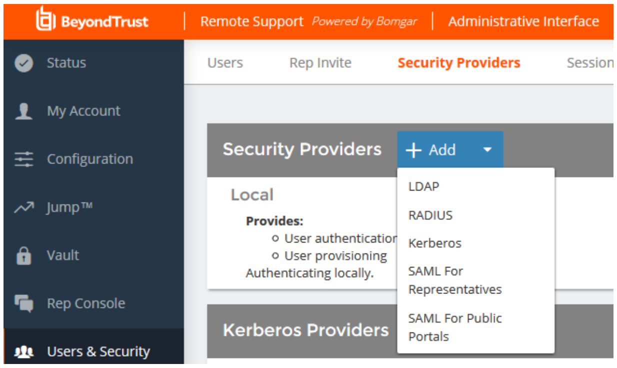
Authenticate Using: Username & Password

English (US)

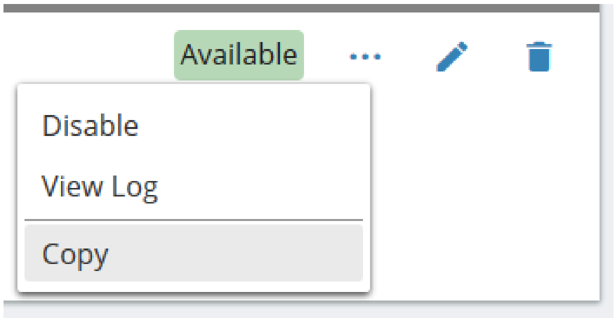
Create and Configure the RADIUS Security Provider

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

Click **Add**. From the dropdown, select the type of server you want to configure.



Alternatively, you can copy an existing provider configuration by clicking the ellipse on a listed provider and then selecting **Copy**.



If you want to copy one node in a cluster, click the ellipse for the node and then select **Duplicate Node**.

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

Name

Create a unique name to help identify this provider.

Enabled

If checked, your BeyondTrust Appliance B Series can search this security provider when a user attempts to log in to the representative console or **/login**. If unchecked, this provider will not be searched.

Keep display name synchronized with remote system

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

Authorization Settings

Only allow the following users

You can choose to allow access only to specified users on your RADIUS server. Enter each username separated by a line break. Once entered, these users will be available from the **Add Policy Member** dialog when editing group policies on the **/login > Users & Security > Group Policies** page.

If you leave this field blank, all users who authenticate against your RADIUS server will be allowed; if you allow all, you must also specify a default group policy.

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 B Series 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.

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.

> ***Note:*** *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.*

Connection Settings

Hostname

Enter the hostname of the server that houses your external directory store.

Port

Specify the authentication port for your RADIUS server. This is typically port **1812**.

Timeout (seconds)

Set the length of time to wait for a response from the server. Note that if the response is **Response-Accept** or **Response-Challenge**, then RADIUS will wait the entire time specified here before authenticating the account. Therefore, it is encouraged to keep this value as low as reasonably possible given your network settings. An ideal value is 3-5 seconds, with the maximum value at three minutes.

Connection Method

If you are using an external directory store in the same LAN as your BeyondTrust Appliance B Series, the two systems may be able to communicate directly, in which case you can leave the option **Proxy from appliance through the Connection Agent** unchecked and move on.

If the two systems are unable to communicate directly, such as if your external directory server is behind a firewall, you must use a connection agent. Downloading the Win32 connection agent enables your directory server and your B Series Appliance to communicate via an SSL-encrypted, outbound connection, with no firewall configuration. The connection agent can be downloaded to either the directory server or a separate server on the same network as your directory server (recommended).

In the case above, check **Proxy from appliance through the Connection Agent**. Create a **Connection Agent Password** for use in the connection agent installation process. Then click **Download Connection Agent**, run the installer, and follow the installation wizard. During installation, you will be prompted to enter the security provider name and the connection agent password you created above.

Shared Secret

Provide a new shared secret so your B Series Appliance and your RADIUS server can communicate.

Save Changes

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

Configuration Specific to Windows 2000/2003 IAS

Each user who will be authenticating with your IAS server must have remote access permission. The remote access permission can be defined via the Active Directory **Users and Computer** snap-in. View the properties for the appropriate user. On the tab **Dial-in**, grant the **Allow Access to Remote Access** permission.

You can also configure this permission through the remote access policy. Please consult your Windows documentation for the proper steps.

IMPORTANT!

The policy must allow for authentication via PAP, as this is the only RADIUS method currently supported by BeyondTrust. Review your IAS policy and ensure this method is supported as a means of authenticating via your BeyondTrust Appliance B Series.

Cluster RADIUS Providers for Load Balancing or Failover

To create a cluster of security providers, first create a security provider configuration for a server you wish to include in the cluster. On the main security providers page, locate this security provider and click the ellipse, and then select **Upgrade to a Cluster**. This creates a cluster with one node. To add more servers to the cluster, click the ellipse and then select **Duplicate Node**. Edit the new node to point to a different server you want in this cluster.

When editing a cluster, you will see a section to modify the cluster settings.

Cluster Settings *(Visible Only for Clusters)*

Member Selection Algorithm

Select the method to search the nodes in this cluster.

Top-to-bottom first attempts the server with the highest priority in the cluster. If that server is unavailable or the account is not found, the next highest priority server is attempted. The search moves down through the list of clustered servers until either the account is found or it is determined that the account does not exist on any of the specified and available servers.

Round-robin is designed to balance the load between multiple servers. The algorithm chooses at random which server to attempt first. If that server is unavailable or the account is not found, another random server is attempted. The search continues at random through the remaining servers in the cluster until either the account is found or it is determined that the account does not exist on any of the specified and available servers.

Retry Delay

Set how long to wait after a cluster member becomes unavailable before trying that cluster member again.

To move a security provider from a cluster to a stand-alone security provider, click the ellipse for the cluster node and then select **Copy**. This copies the settings to a new, top-level security provider. You can then delete the originating node.

Test the Settings of the RADIUS Integration

After entering configuration settings for a security provider, test the configuration at the bottom of the security provider's edit page.

Test Settings

Username and Password

Enter a username and password for an account that exists on the server you are testing. This account must match the criteria for login specified in the configuration above.

Try to obtain user attributes and group memberships if the credentials are accepted

If this option is checked, your successful credential test will also attempt to check user attributes and group lookup.

> ***Note:*** *For these features to be successfully tested they must be supported and configured in your security provider.*

Test

If your server is properly configured and you have entered a valid test username and password, you will receive a success message. Otherwise, you will see an error message and a log that will help in debugging the problem.

> ***Note:*** *When testing a cluster, the cluster will test its member servers according to its operating mode, either in order or priority or at random. If the first attempted server is properly configured and you have entered a valid test username and password, you will receive a success message. Otherwise, the cluster will attempt the next security provider.*
>
> *If the test username and password properly bind to any of the servers, you will receive a success message, even if the other servers are improperly configured. You will receive an error message only if you are unable to bind to any of the clustered servers.*

> *For more information, please see "Troubleshoot RADIUS Server Integration Errors" on page 14.*

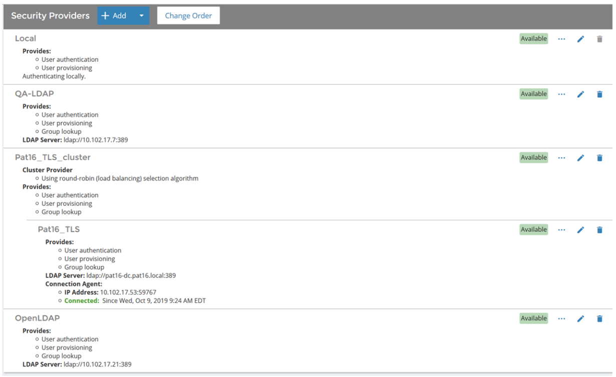
Prioritize and Manage Security Providers: RADIUS Servers and Others

Change Order

Once you have set up your security providers, you can configure the order in which your B Series 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 Order** button.



Local

Provides:
- User authentication
- User provisioning

Authenticating locally.

QA-LDAP

Provides:
- User authentication
- User provisioning
- Group lookup

LDAP Server: ldap://10.102.17.7:389

Pat16_TLS_cluster

Cluster Provider
- Using round-robin (load balancing) selection algorithm

Provides:
- User authentication
- User provisioning
- Group lookup

Pat16_TLS

Provides:
- User authentication
- User provisioning
- Group lookup

LDAP Server: ldap://pat16-dc.pat16.local:389
Connection Agent:
- **IP Address:** 10.102.17.53:59767
- **Connected:** Since Wed, Oct 9, 2019 9:24 AM EDT

OpenLDAP

Provides:
- User authentication
- User provisioning
- Group lookup

LDAP Server: ldap://10.102.17.21:389

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.

Disable

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

View Log

View the status history for a security provider connection.

Troubleshoot RADIUS Server Integration Errors

Failed Logins

The best way to troubleshoot a failed login is to test the settings in the security provider's configuration page. The section below helps you to understand the messages you may receive.

If testing a username and password from the **Security Providers** page provides no errors but the user cannot log in to BeyondTrust using those same 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.

Message 1: Authentication Failed

1. The username and password that you are testing do not match.
2. Reenter the credentials or attempt another username and password.

Message 10: Server Unavailable

1. Your DNS information may be incorrect. You can test if your DNS server resolves by using the tools on the **Support > Utilities** page in your BeyondTrust /appliance interface.
2. You must use the correct shared secret between RADIUS and your B Series Appliance.
3. If a user who can normally authenticate cannot connect, check if the user's hours are restricted on the RADIUS server.
4. If you are using an IAS server, the user authenticating must have remote access permission enabled.
5. Authentication via PAP must be enabled. This is the only RADIUS method currently supported by BeyondTrust. Edit your IAS policy and ensure this method is supported as a means of authenticating via the B Series Appliance.

Error 6ca and Slow Logins

1. A **6ca** error is a default response signifying that the B Series Appliance has not heard back from the DNS server. It may occur when attempting to log in to 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 user authentication first, 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. 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.