MENU

Search

Search

Carbon Black Cloud AuthHub Migration FAQ

Article ID: 383516 Updated On: 01-22-2025

Products

Carbon Black Cloud Endpoint Standard (formerly Cb Defense)

Carbon Black Cloud Audit and Remediation (formerly Cb Live Ops)

Carbon Black Cloud Enterprise EDR (formerly Cb Threathunter)

Carbon Black Cloud Managed Detection (formerly Cb Threatsight)

Carbon Black Cloud Managed Threat Hunting

Carbon Black Cloud Managed Detection and Response

Carbon Black Cloud Prevention

Carbon Black Cloud Workload

Issue/Introduction

This knowledge base article is intended for Carbon Black Cloud Super Admin that will perform the user authentication migration to AuthHub.

Non-Federated

- This is for customers who are not currently using 2FA / SAML (using a single set of credentials at login).

ederated

- This is for customers who are currently using 2FA / SAML.

Managed Service Provider (MSSP)

- For environments that are configured as an MSSP with Carbon Black Cloud

Cause

As we previously announced, Carbon Black Cloud is migrating it's user authentication to AuthHub.

Resolution

Table of Contents

Non-Federated (Not using 2FA/SAML):

Q: When does my migration begin and what migration steps are necessary?

A: Early adopters can begin migrating their user authentication to AuthHub on December 16th. For those who prefer to wait until after the holiday season, the migration window will continue to be available from January 21st to April 28th, 2025. Note that the in-product banner to begin the

migration will not appear for all customers on January 21. This is a phased rollout and we expect all customers to have the banner no later than February 7th.

For migration steps, see the Broadcom Community Post.

Q: Now that Multi-Factor Authentication is mandatory and Duo Security is no longer supported, what are my options?

A:

- **Email** OTP
- Use **biometrics**
- Use code from **mobile app**

When choosing a mobile app as an authenticator, you will be prompted to set up Broadcom's VIP Access app. Using the VIP Access app will now allow you to use push notifications instead of entering the code manually.

However, if you currently use Google Authenticator (or another similar OTP application) and wish to continue using this method please select "Use another app" and scan the QR code with Google Authenticator (or your preferred OTP application)

Federated (Using 2FA/SAML integration):

Q: When does my migration begin and what migration steps are necessary?

A: Early adopters can begin migrating their user authentication to AuthHub on December 16th. For those who prefer to wait until after the holiday season, the migration window will continue to be available from January 21st to April 28th, 2025. Note that the in-product banner to begin the migration will not appear for all customers on January 21. This is a phased rollout and we expect all customers to have the banner no later than February 7th.

For migration steps, see the Broadcom Community Post.

Q: Prior to the migration window opening, I am unable to create a new 2FA/SAML integration in Carbon Black Cloud. Could you please assist me in resolving this issue?

A: New SAML creation has been disabled until user authentication migrates to Broadcom's AuthHub to prevent unnecessary re-work. However, if you have an urgent need, please open a support case and include your Org Key.

Q: Can other users be in the console while I am performing the migration?

A: Other users can be logged into the console at the same time the migration is happening. When the other users' sessions end or they logout, they will have to authenticate with the IdP (same as they did before.)

Q: What happens if I start the AuthHub migration but then have to resume later?

A: If you stop before validating trust configuration by signing back into CBC, you will have to start the migration steps from the beginning.

A: If you stop the migration steps after you have validated trust configuration by signing back into CBC, you can either authenticate and press “Complete Migration” or start the revert process.

Q: In order to verify ownership of a domain, how do I add a new verification record to my domain’s DNS settings at the organization’s domain host?

A:

1. In the wizard your specific domain’s TXT name and TXT value can be found.
2. Log in to your domain registrar and look for sections labeled “DNS,” “Name Servers,” or something similar.
3. Add a new TXT record.
4. Paste the TXT name and value from the Carbon Black wizard.
5. Save the changes. Changes may take up to 24 hours.
6. Return to Carbon Black’s UI wizard to check that your domain now displays as verified.

Q: Why do I need to create a “recovery local user?”

A: You are strongly urged to create a temporary local user as a recovery mechanism in case an error occurs when you configure your IdP trust to AuthHub. This local user will be deleted after your migration is complete.

SAML Configuration Error Occurs:

Q: After I create a new application entry in my IdP, how will I know if an error has occurred?

A: After you configure your trust within the IdP and sign out of CBC and log back in using your typical super admin credentials, then an error has occurred. Login using your recovery credentials to revert the migration and begin again.

Q: If I am unable to login to CBC using my super admin credentials, what happens next?

A:

Instead, login to CBC using your local recovery user. Go to Settings > Users > Revert Migration. If a revert is necessary, please check the following before retrying the migration:

- Is the domain correct?
- Does the super admin have the correct domain?
- Copy and paste the trust credentials into the IdP again

If the issue still persists, open a support ticket.

Q: How do I know if “Revert Migration” was successful?

A: If you are able to login using your super admin credentials, the revert was successful.

Managed Service Provider (MSSP):

Q: Will MSSP users be able to login to access their current SSO configuration, or will they need to reconfigure authentication via AuthHub?

A: MSSP orgs are no different than other orgs in this respect.

- If the org is federated, its Super Admin needs to go through the migration wizard.
- If the org is not federated (i.e. local users), each user needs to reset their password.

Feedback

Was this article helpful?

Yes No