blue cedar

DATA SHEET

PLATFORM SECURITY POLICIES

The Blue Cedar Platform offers you many powerful and flexible policies with which to secure your apps and data, and govern how users are allowed to access them.

CERTIFICATE MANAGEMENT

The Blue Cedar Platform provides an easy enrollment experience for an end user to get a digital certificate from your PKI. Blue Cedar brokers secure communication with your PKI and makes the entire process of enrollment, expiration/renewal, revocation, and trusted server certificate management completely transparent to the end user.

Client Certificates

The client certificate can be presented to web servers and used to skip login prompts from web servers, resulting in a smoother mobile experience.

The policy allows you to use URL patterns to specify a White List of sites to whom the app can present the client certificate. That White List can be superseded by an Exception List of sites where you explicitly do not want the certificate presented.

Trusted Server Certificates

Allows definition on a per-app basis of a list of trusted root, intermediate, and server certificates. Users going to sites presenting a trusted certificate will not be prompted to manually trust the site.

NETWORK INTEGRATION

Blue Cedar provides powerful tools to control how users and apps are able to connect to your network to consume your data, whether it lives in an on-premises data center or in the cloud.

Secure Web Stack

PROXY SERVER

Control how an app connects to its back-end service or application:

- Direct connection
- Specified Proxy Server(s)
- PAC file

SSO INTEGRATION

The Blue Cedar Gateway retrieves and stores cookies/session credentials from your SSO system and passes them onto any websites that are protected using that SSO system. This maintains your security posture while preserving the SSO experience for the end user.

BRANDING

Branding is a crucial element for both brand integrity and security behavior reinforcement. The App Customization policy gives you many different ways to brand the user-facing elements and screens used for enrollment, authentication, and other Blue Cedar functions.

Background

The screen background can be customized as follows:

- Specify color (via color menu or Hex)
- Upload an image to be used as the background

Logo

Provide your logo to be displayed on enrollment, authentication, and other screens.

Secondary Colors

You can separately configure complementary/accent colors for primary buttons and secondary buttons.

Translation strings

Customize the text that appears to app users, using translated strings for the device locale or your organization’s terminology.

SECURE ACCESS (Data-in-Transit Security)

Blue Cedar enables each secured app to create a dedicated **Secure Microtunnel** to its back-end service or application. This is an IPsec VPN where the client is embedded into the app itself, making the entire secure connectivity aspect completely transparent to the end user. This is sometimes also called a "Per-App VPN." We prefer the term Secure Microtunnel because—unlike most solutions where apps actually share a common device-level VPN—Blue Cedar creates a discrete secure connection from each app, delivering significant usability and security benefits for you and your end users.

VPN Server

Specify which Blue Cedar Gateway(s) the app is allowed to connect to.

Authentication Method

Configure mechanisms by which users can authenticate and connect to the Blue Cedar Gateway.

- Digital Certificate: Use the pre-enrolled certificate and make the authentication transparent to the end user.
- Pre-Shared Key (PSK): Pre-specified at wrapping time, or configured to have the user enter it when attempting to connect.

Authentication Groups

Specify different authentication groups for different types of users. This allows you to configure different security features and levels for different groups of users, such as executives, employees, and contractors.

Managed Devices

Device must be managed by your MDM/EMM solution. If unmanaged, the app will not connect.

Offline Use

Allows the app to be used locally even when unable to connect to the Blue Cedar Gateway. Ideal for apps that have native functionality and local data storage that allow users to continue to be productive when airborne, underground, or otherwise offline.

DATA-AT-REST SECURITY (DAR)

The **Encrypted Data-at-Rest** policy strongly encrypts each piece of app data before saving it on the mobile device, shielding the data from malware, rogue apps, and hackers who attack the device storage. When the app needs an encrypted piece of data, the DAR policy decrypts it.

FIPS 140-2

Blue Cedar uses FIPS-certified cryptography. When enabled, this policy ensures that all secure connectivity, all data-at-rest cryptography, and all local app authentication is handled using FIPS-certified algorithms.

COMPASS SECURE BROWSER

The Compass Browser is a special app that allows a user to securely access any websites that your organization permits. You can customize it with the Browser Configuration policies:

Launch Pad

Pre-configure a Launch Pad with icons for the websites you want your users to be able to access.

URL Entry

Specify if users are permitted to enter URLs other than the ones you make available via the Launch Pad.

Search

If URL Entry is permitted and the user enters an invalid URL into the address bar, this policy lets you allow/disallow performing a Google search on the string.

History

Allow/Disallow users to view and navigate to previously visited sites.

Bookmarks

Allow/Disallow users to bookmark sites.

Email

Allow/Disallow users' ability to share the web page via email.

Branding

You can brand Compass in the following ways:

- Icon
- Name (e.g., *YourCompany* Secure Browser)
- Theme Color
- Home Page (if none specified, the user sees the Launch Pad)

LOCAL APP SECURITY

The Local App Authentication set of policies allow rich and granular control over how the user authenticates locally to the app. This ensures that the app and its encapsulated data are secure even when offline or if the device has been lost or stolen.

Security Method

Specify whether local authentication should require a PIN or a Passphrase.

Fingerprint

Allow users to authenticate using fingerprint authentication.

Minimum PIN/Passphrase Length

Require a minimum length for the PIN or Passphrase.

Re-Authentication

Specify if you want the user to re-authenticate each time the app is launched or returned to the foreground from an idle state.

Unattended Login

Specify if you want the user to re-authenticate each time the app is launched or returned to the foreground from an idle state.

Idle Timeout

Configure the amount of inactive time after which the user is forced to re-authenticate to the app.

Require Special Characters

For Passphrase authentication, you can require the passphrase to contain one or more of the following:

- Alphabet
- Lowercase letters
- Uppercase letters
- Numerals
- Special characters

Passphrase/PIN History

The user cannot repeat a previously used PIN or passphrase.

Passphrase Aging

The user must periodically change their passphrase. This policy allows you to configure the interval at which the user must change their passphrase, and when to remind the user.

Passphrase/PIN Complexity

The user must select a complex passphrase or PIN. Complex passphrases may not contain four or more of each of the following:

- Same number and/or character, for example: 111111, abbbbc, 8888xyz
- Numbers and/or characters in sequence (including reverse), for example: 123456, 8765ab, abcde1928
- Any sequence of numbers (including reverse) with the same interval, such as odd/even numbers, for example: 1357xxx, 8642000, 036999

Lockout

Specify the number of failed login attempts after which to lock the user out.

DEVICE POSTURE

The Device Posture policy allows you to enforce device posture attributes before allowing a secured app to launch or come to the foreground.

Minimum OS Version

Specify minimum version of device operating system below which the app will not launch or run.

Device Screen Lock

Device must have PIN, password, or pattern set up before the secured app will launch or run.

Jailbreak/Rooting

Prevent app from launching or running if device is jailbroken or rooted.

DATA LOSS PREVENTION (DLP)

For apps that handle sensitive data, the **Data Sharing** policy prevents corporate data leakage by allowing you to constrain what kind of data users can share between a protected app and another app.

- Copy and paste between a protected app and another app.
- Open links and attachments in preferred external apps.
- Use a privacy screen to block app screens from appearing in the app switcher.
- Use grouped apps to share credentials and encryption keys with affiliated apps.

MASTER PROFILES

A Master policy profile is a collection of individual policy profiles. You can use a master profile to provide a streamlined way to wrap multiple apps with a consistent set of policies.

DIAGNOSTICS

The Diagnostics policy allows you to configure logging for the Blue Cedar Platform at six verbosity levels for each of the areas specified below.

Blue Cedar logs everything via Syslog where you can use your internal tools to gather Blue Cedar logs and, if desired, aggregate them with other logs for troubleshooting, forensics, operational intelligence, and security intelligence.

Certificate Enrollment

Initial registration and enrollment.

Client

High-level logs related to all activity from a secured app to the Blue Cedar Gateway.

Authentication

Attempted authentications, including success/failure, lockouts, etc.

Crypto

Cryptography and security services, including FIPS.

HTTP

Information from interception layer for web traffic (HTTP/HTTPS).

Policy

Information and debug on static and dynamic Blue Cedar Policy, including secure microtunnel settings, browser settings, and device posture.

FileIO

File System interactions.

Various

The above list is not exhaustive. There are numerous other Blue Cedar subsystems for which logging can be turned on, but typically these are used under direction from Blue Cedar's support team and used for troubleshooting purposes.

ABOUT BLUE CEDAR

Blue Cedar transforms enterprise mobility with the industry's most innovative mobile security solution. By securing the app rather than the device, Blue Cedar gives enterprises robust, consistent protection of corporate data across both managed and unmanaged devices, without the cost, complexity, or privacy impact of device-level security. Blue Cedar's "follow the app" security sets enterprises free to fully realize the benefits of secure mobility for both employees and customers.