Application Access Control

Mobile Connect 4.0 and higher supports the Application Access Control feature in SonicWall Secure Mobile Access 11.0 and higher on SonicWall SMA 1000 Series / E-Class SRA appliances.

Topics:

- About Application Access Control
- Logging in and Registering your Device
- Controlling App Behavior
- Viewing the App List after Connecting
- About Learning Mode (Administrators Only)

Related topics:

- Introduction to Mobile Connect
- Installing and Connecting
- Settings, Bookmarks, and Files
- Monitoring and Troubleshooting
- SonicWall Support

About Application Access Control

Application Access Control allows remote access administrators to control exactly which resources on the corporate network each application (app) can access. Meanwhile, the device owner can still use their personal Android device for their own activities such as personal email, financial data, pictures, music, accessing third party web sites, etc.

If the SMA 1000 Series / E-Class SRA administrator has configured this feature, you will log in to a Login Group that allows a list of trusted apps to access corporate resources. The specific version of each app is included in the configuration.

The Application Access Control rule list controls the following:

- Which applications can send data through the VPN tunnel
- Which destinations on the corporate network those applications are allowed to access

When connected to a SonicWall SMA 1000 Series / E-Class SRA server running SonicWall Secure Mobile Access 11.0 or higher with Application Access Control configured, device traffic is handled in four ways:

1. For applications listed and selected in the application list, traffic destined for the corporate network from those applications is allowed to enter the VPN tunnel. The application ID and signature are used by the server to identify the application.
2. For applications that are on that list and are not selected (or any other application on the device), traffic destined for the corporate network is blocked and/or dropped by Mobile Connect and does NOT enter the tunnel.
3. All applications (regardless of whether or not they are on the application list) send traffic out the default interface of the device if the traffic is NOT destined for the corporate network.
4. The information status symbol ‘i’ displays on applications that are learned by the appliance but still have at least one version pending approval.

Logging in and Registering your Device

The first time you connect and log in, you must agree to the displayed terms and conditions. These include:

- The device belongs to you and is not a shared device.
- You will comply with all corporate policies.
- You will keep the device credentials safe.
- The device identifier can be collected and stored by the server administrator.

Agreeing to terms

Authorize your device

Before you are permitted to use this device to access the VPN network you must agree to the following:
1. This device belongs to you and is not a shared device or a public kiosk type device.
2. You will comply with all corporate policies regarding access of company data and resources from this personal device.
3. You will always keep the credentials for this device safe.

As part of this authorization process, a unique identifier of your device will be collected and stored by your administrator. This unique identifier is verified every time you log in to the VPN network. The company will not share information coming from your personal device with entities outside the corporation unless legally required to do so.

Do you agree to these terms and conditions? If you do not or cannot agree to these terms and conditions, please log out now.
To agree and continue, tap ACCEPT.

Your device is then registered with the server, and will be recognized in later connections.

Multiple personal devices can be authorized for a single user, and a single personal device may be registered by multiple users.

If the policy or list of trusted apps changes, you are asked to re-accept the terms and conditions.

Changes in terms or trusted apps

To agree and continue, tap ACCEPT.

Related topics:

- Application Access Control
- Controlling App Behavior
- Viewing the App List after Connecting
- About Learning Mode (Administrators Only)

Controlling App Behavior

The list of trusted apps is displayed on your device after you agree to the terms and conditions.

NOTE: To request that additional apps be added to the trusted apps list, contact the SonicWall SMA 1000 Series / E-Class SRA appliance administrator.

Trusted app list

To control app behavior:

1. Clear the checkbox next to the app to prevent the app from sending data to the corporate network.
Typically, you would do this for any application that is only being used for personal tasks or information.

2 Tap ACCEPT to continue with the connection to the SMA 1000 Series / E-Class SRA server.

Related topics:

- Application Access Control
- Logging in and Registering your Device
- Viewing the App List after Connecting
- About Learning Mode (Administrators Only)

### Viewing the App List after Connecting

The Application Control section of an active connection screen displays the list of apps that are known by the server.

#### App list with mixed status

![App List Screenshot](image)

A status indicator is displayed next to each app.

- A check mark ✅ indicates that the app is installed on your device and is permitted to access the corporate network.
- A red circle with a slash ⌃ indicates one of the following conditions:
  - The version of the app on your device is not the same as the approved version in the server.
  - The app is approved by the server, but it is not installed on your device.

Tapping the Application Control help icon ![Help Icon](image) displays information about Application Control. Tap OK to exit the help screen.

#### Application Control help

![Help Screen Screenshot](image)

Related topics:
About Learning Mode (Administrators Only)

Designated administrators can use Android devices as trusted learning devices when working with SonicWall SMA 1000 Series / E-Class SRA appliances running Secure Mobile Access 11.0 and higher with Application Access Control enabled. A trusted learning device is assigned special privileges to perform signature lookups as a part of the process of learning application version information. When the trusted learning device is connected to the SMA 1000 Series / E-Class SRA server, apps that need versions to be learned are displayed. After launching the app, a “!” “pending approval” icon displays next to the app name. The app can then be approved by the SMA 1000 Series / E-Class SRA administrator.

For more information about configuring Application Access Control on the SMA 1000 Series / E-Class SRA appliances running SMA 11.0 and higher, see the SonicWall Secure Mobile Access Application Access Control Feature Guide, available on the SonicWall Support portal.

Related topics:
- Application Access Control
- Logging in and Registering your Device
- Controlling App Behavior
- Viewing the App List after Connecting