Security White Paper

Last Modified on 02/11/2021 10:56 pm EET

Carillon security is build in different layers that can be made even more secure using native Microsoft platform features like certificate authentication, SQL database encryption etc. By default all Carillon communications between Carillon components are secure and communications that happen over untrusted networks are protected by Carillon with static encryption even if for example SSL would not be used on network communications.

> **Note!**
>
> Tables in this document containing description of network traffic protocols and ports only include communications required by Carillon components. Other communications (for example ports required to be open for on-prem domain joined devices) are not listed.

SQL Database

Carillon SQL database should be located on trusted network and only Carillon server side component (Carillon Management Portal and Centero Agent Gateway) need to access the SQL database. It's recommended to use Windows authentication when ever possible with Carillon. Centero Management Portal and Centero Agent Gateway web sites application pools are accessing the SQL database and by default using Network Service identity for the access. This can be changed also to SQL login or different Windows based service account. SQL login is used by default when Carillon is running on Azure App Service. Identity that is used in web sites required only Connect permission to SQL instance and to Carillon database rolePortals and/or roleGateways are required from database user. You should not grant sysadmin permissions to SQL login or db_owner role to database user.

As all the configuration on Carillon environment is located on SQL database, that is the most important component to protect. So make sure that unauthorized access directly to the database (or it's backups) is not allowed. If required additional Microsoft SQL features like column data encryption can be taken in to use to give more protection to for example possible endpoint local account random passwords that are stored to database using static encryption by default.

Carillon specific traffic	Protocol and port	Direction	Used by
SQL	TCP/1443 by default but can be different depending of the SQL instance configuration	Inbound	Carillon web sites

Carillon Web Sites

Web sites only contain application functionality and all the data is stored on SQL database. Both web sites have local log files available for tracking actions performed on these web sites. SQL database contains reports for created activation codes for temporary account activation, actions for randomized local account password and information of the current local groups/members and users on all devices where Carillon client is installed.

Both web sites should be protected with SSL certificates so using HTTPS communications. Internal PKI

certificates can be used as long as the devices trust the internal PKI root and intermediate CA's. All web site configurations are stored in web.config file that is protected by the IIS service.

Carillon Management Portal is using Windows Integrated authentication by default for on-prem implementations and Azure AD authentication for Azure App Service implementation. Access to Carillon Management Portal is managed by using on-prem Windows groups (local or on-prem AD) for on-prem implementations and Azure AD Enterprise Application for Azure App Service implementations. Any additional security features from the Microsoft platform (IIS for on-prem implementations and App Service+Azure AD authentication) can be used to more protect Carillon web sites.

Centero Agent Gateway contains web services that Carillon clients will access and also REST API for performing actions (not all actions yet available through REST API) in Carillon Management Portal UI using industry standard REST API. Centero Carillon REST API supports key and Windows Integrated authentication for on-prem implementations. Key and Azure AD authentication is available for Azure App Service implementations.

Carillon clients that communicate to Centero Agent Gateway do not have by default any user identity available for authentication. This is because by default Centero Agent -service that runs on client as Windows service, is running with SYSTEM identity. If user identity is required for authentication to Centero Agent Gateway then Centero Agent -service must be changed to run with this identity. This change is only supported on on-prem implementations as Azure AD authentication is not available for devices.

Carillon specific traffic	Protocol and port	Direction	Used by
HTTP or HTTPS	TCP/80 or TCP/443 by default but can be different depending of the web site configuration	Inbound	Carillon clients REST API calls
LDAP	TCP/389 or TCP/636	Outbound	Connections to on-prem Active Directory domain controllers
HTTPS	TCP/443	Outbound	Connections to Azure AD authentication and Graph API

Carillon Clients

Clients run Windows service that uses SYSTEM identity by default. This service is used to make all changes on the device (like modifying local groups etc.) so service identity must have admin access to the device. All changes made by Carillon to the device is logged to local log file (default location is %ProgramData%\Centero\Agent\Logs\Centero Carillon action.log).

Communication to Centero Agent Gateway is always statically encrypted (in addition of possible SSL encryption) and check for new client configuration is done every hour by default (can be changed). Communication is always opened from the client to Centero Agent Gateway. So Centero Agent Gateway does not open any communication to client. Communications can be additionally protected by using client certificates for web site authorization.

Client configuration received from Centero Agent Gateway is cached to client registry as encrypted value. This cache is used to validate and maintain desired configuration on client and cached configuration is validated every 5 minutes (can be changed). Local user account password are never saved to cache and configuration

received from Centero Agent Gateway can contain password information only if Carillon administrator has created configuration rule that uses fixed password.

Carillon specific traffic	Protocol and port	Direction	Used by
HTTP or HTTPS	TCP/80 or TCP/443 by default but can be different depending of the web site configuration	Outbound	Centero agent service on client