Privilege Manager Security Overview

Last Modified on 12.01.22

Privilege Manager security is built 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 communications between Privilege Manager components are secure and communications that happen over untrusted networks are protected by Privilege Manager with static encryption even if, for example, SSL would not be used on network communications.

NOTE: Tables in this document containing descriptions of network traffic protocols and ports only include communications required by Privilege Manager components. Other communications (for example, ports required to be open for on-premises domain-joined devices) are not listed.

SQL Database

The Privilege Manager SQL database should be located on a trusted network and only the Privilege Manager server side component (Privilege Manager Management Portal and Recast Agent Gateway) need to access the SQL database. It's recommended to use Windows authentication whenever possible with Privilege Manager. Privilege Manager Management Portal and the Recast Agent Gateway website application pools are accessing the SQL database and by default using Network Service identity for the access. This can also be changed to SQL login or different Windows-based service accounts. SQL login is used by default when Privilege Manager is running on the Azure App Service. Identity that is used in the websites require only Connect permission to the SQL instance and to the Privilege Manager database role Portals and/or role Gateways are required for the database user. You should not grant sysadmin permissions to SQL login or db_owner role to database user.

As all the configuration for the Privilege Manager environment is located on the SQL database, that is the most important component to protect. Ensure that unauthorized access to the database (or its 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.

Privilege Manager specific traffic	**Protocol and port**	**Direction**	**Used by**
SQL	TCP/1443 by default but can be different depending on the SQL instance configuration	Inbound	Privilege Manager websites

Privilege Manager Web Sites

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

Both websites 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 CAs. All website configurations are stored in the web.config file that is protected by the IIS service.

By default, the Privilege Manager Portal uses Windows-integrated authentication for on-premises implementations and Azure AD authentication for Azure App Service implementation. Access to the Privilege Manager Portal is managed by using on-premises Windows groups (local or on-premises AD) for on-premises implementations and Azure AD Enterprise Applications for Azure App Service implementations. Any additional security features from the Microsoft platform (IIS for on-premises implementations and App Service+Azure AD authentication) can be used to more protect Recast websites.

Recast Agent Gateway contains web services that Privilege Manager clients will access and also a REST API for performing actions (not all actions yet available through REST API) from the Privilege Manager Portal interface using an industry-standard REST API. The Recast Software Privilege Manager REST API supports key and Windows-integrated authentication for on-premises implementations. Key and Azure AD authentication is available for Azure App Service implementations.

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

Privilege Manager-specific traffic	**Protocol and port**	**Direction**	**Used by**
HTTP or HTTPS	TCP/80 or TCP/443 by default but can be different depending on website configuration	Inbound	Privilege Manager 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

Privilege Manager Clients

By default, clients run a Windows service that uses SYSTEM identity. This service is used to make all changes on the device (such as modifying local groups etc.) so the service identity must have admin access to the device. All changes made by Privilege Manager to the device are logged to the local log file located at `%ProgramData%\Recast\Agent\Logs\Privilege Manager action.log`.

Communication to the Recast Agent Gateway is always statically encrypted (in addition to possible SSL encryption) and a check for new client configuration is done every hour by default (can be changed). Communication is always initiated by the client to the Recast Agent Gateway, meaning that the Recast Agent Gateway does not open any communication to the client. Communications can be additionally protected by using client certificates for website authorization.

Client configurations received from the Recast Agent Gateway are cached to the client registry as encrypted values. This cache is used to validate and maintain desired configurations on client and cached configuration is validated every 5 minutes (can be changed). Local user account passwords are never saved to the cache and configuration received from the Recast Agent Gateway can contain password information only if a Privilege Manager administrator creates a configuration rule that uses fixed passwords.

Privilege Manager specific traffic	**Protocol and port**	**Direction**	**Used by**
HTTP or HTTPS	TCP/80 or TCP/443 by default, can be different depending on website configuration	Outbound	Recast agent service on client