What additional requirements are there for On-Premises installation?

Last Modified on 09/11/2026 11:11 am EDT

Additional On-Premises Requirements

Windows IIS Application Server Requirements

The physical or virtual application servers must meet the following baseline checklist:

- **Operating System:** Windows Server 2019 (64-bit) running IIS 10 with full Microsoft .NET 4.8 components installed.
- **SSL Bindings:** A public SHA-256 SSL Certificate must be bound to port 443. This is required for secure HTTPS client communication, manifest routing, and metrics payload delivery. If the server is strictly internal, a self-signed or internal CA certificate is permissible, provided client endpoints trust it.
- **DNS and Trusted Sites Zone:** The server hostname should be structured as a third-level subdomain of your primary corporate domain (e.g., pm.yourcompany.com). To prevent Outlook browser errors and image rendering blocks on the client, the server hostname must reside within your Active Directory Internet Explorer Trusted Sites Zone, pushed via Group Policy Object (GPO).

Required Service Accounts & Permissions

Administrators must configure four specific types of service accounts to allow secure inter-component communication and prevent outages caused by password rotations:

- **Server Service Account:** Used to run local software installations, updates, and server tools. This account requires local Administrator rights on the IIS host. It must also have read/write/execute permissions on the PoliteMail database files to perform updates without requiring a Database Administrator (DBA) present.
- **SQL Service Account:** The primary account utilized by the IIS Application Pool to write metrics to SQL. It can use either Windows Authentication or SQL Server Authentication and requires read/write/execute/control permissions to the databases.
- **gMSA (Group Managed Service Account):** gMSA is highly recommended in lieu of standard SQL Windows accounts. Password rotation is managed automatically via the Active Directory Domain Controller via Kerberos, completely eliminating database communication outages caused by expired service credentials.
- **EWS Service Account:** Used strictly for authenticating EWS list expansion processes against Exchange. This must be a mail-enabled Active Directory object with a standard Exchange mailbox and view membership rights on nested and dynamic distribution lists.