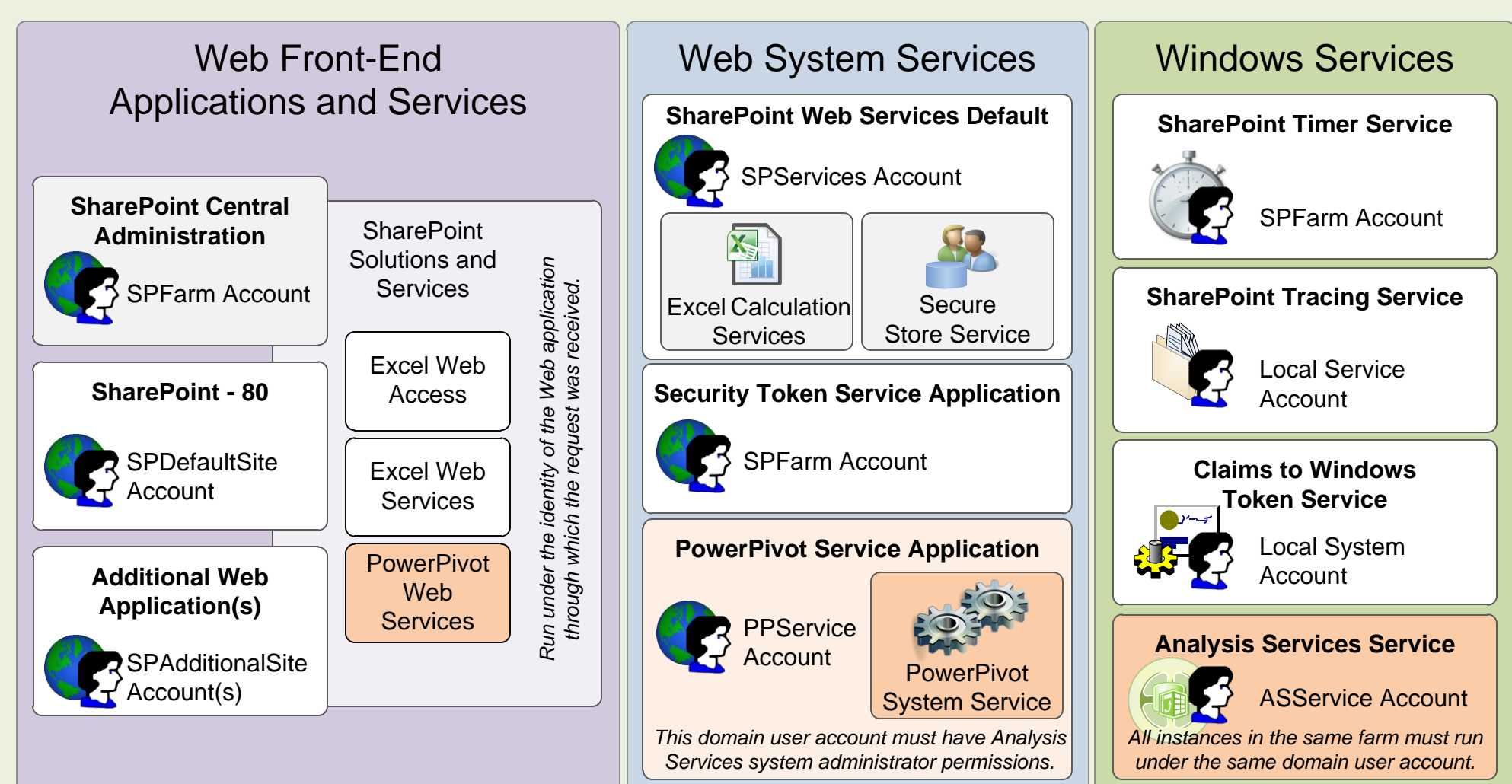


PowerPivot Security Architecture



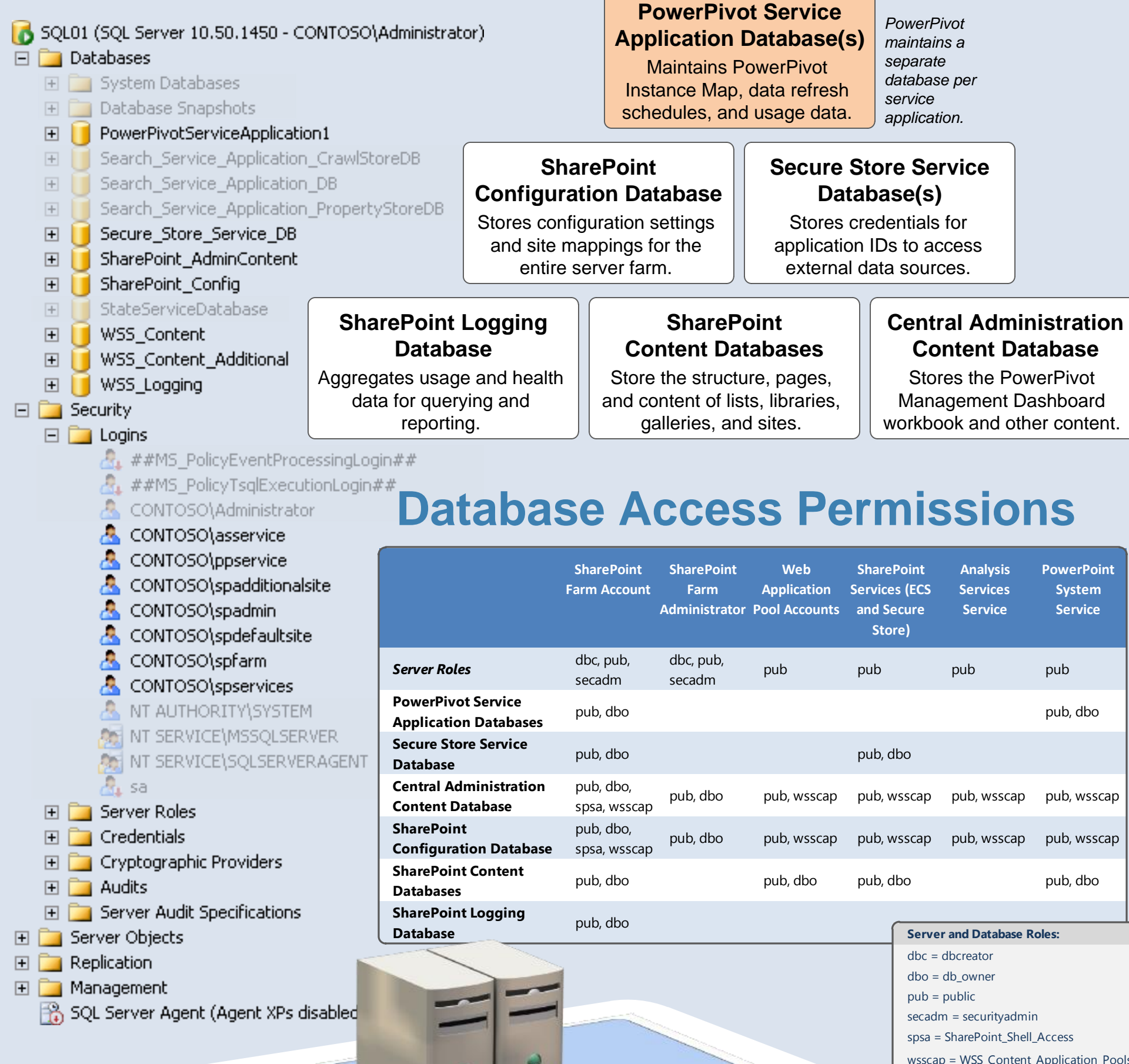
Service Accounts

In addition to the standard service accounts for Web applications and SharePoint services, PowerPivot for SharePoint requires two service accounts: one account for the PowerPivot System service application and the other for the SQL Server Analysis Services service.



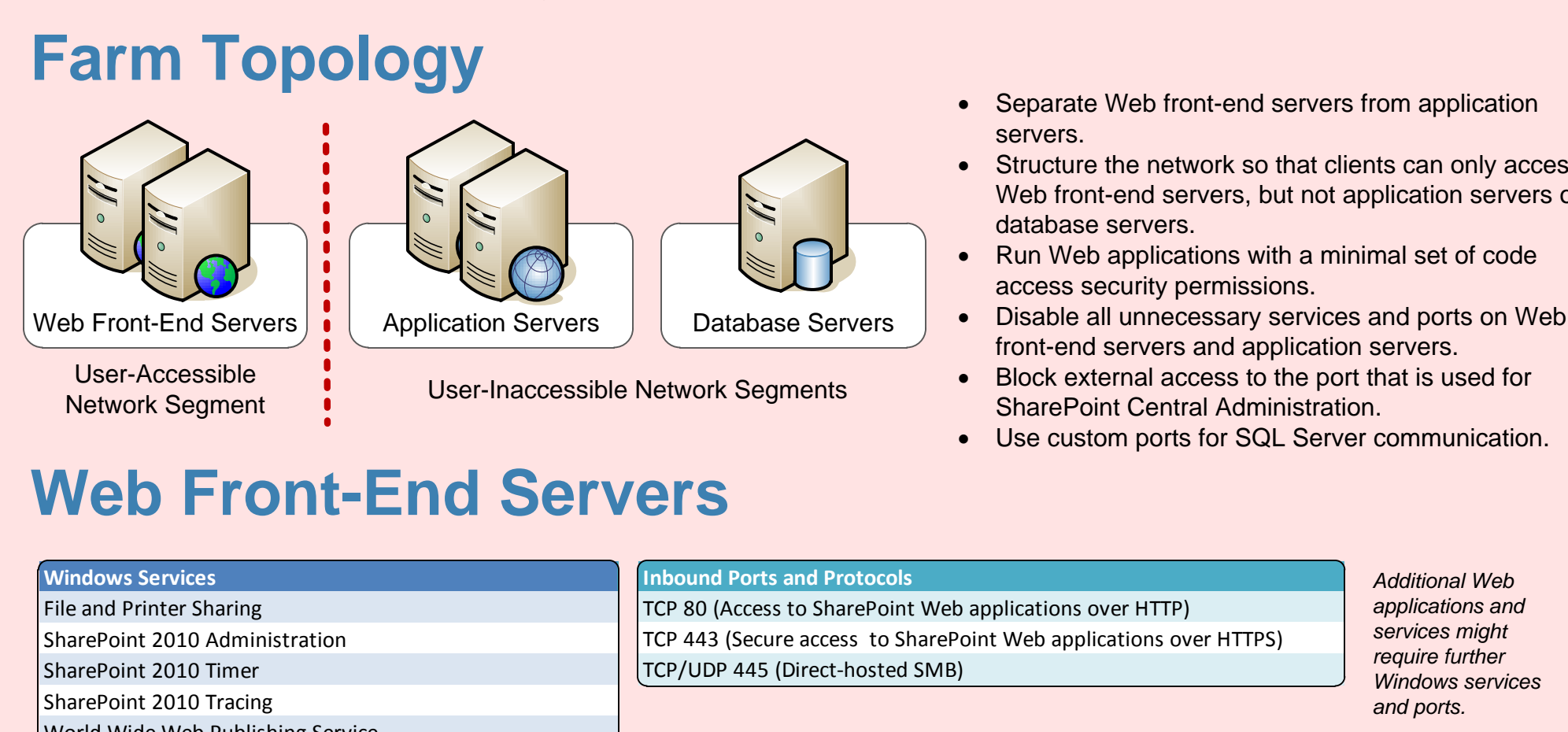
SharePoint Databases

SharePoint stores PowerPivot configuration settings, usage and health data, unattended data refresh credentials, and PowerPivot workbooks in its databases. Each PowerPivot service application also uses its own database to maintain internal application data.

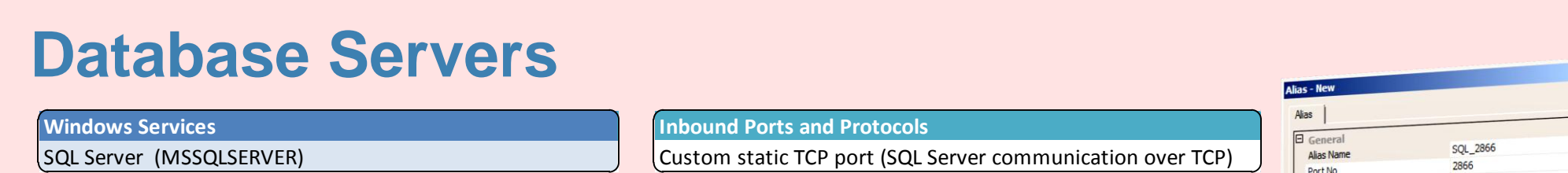
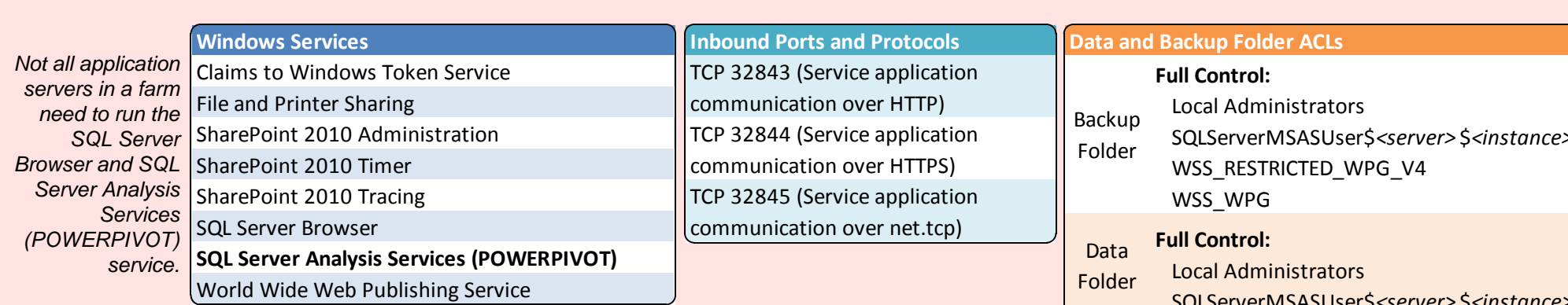


Security Hardening

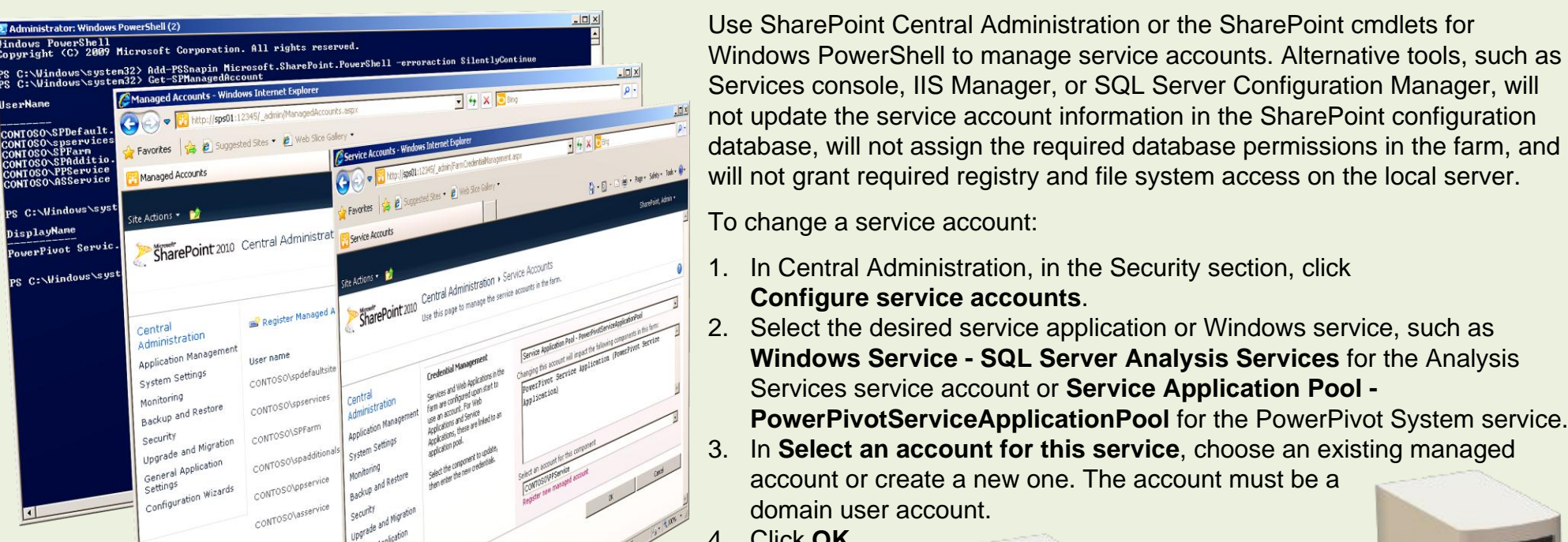
PowerPivot for SharePoint has no special security hardening requirements. The standard SharePoint recommendations apply, as outlined in the section "Plan Security Hardening" on Microsoft TechNet at <http://technet.microsoft.com/en-us/library/cc262849.aspx>.



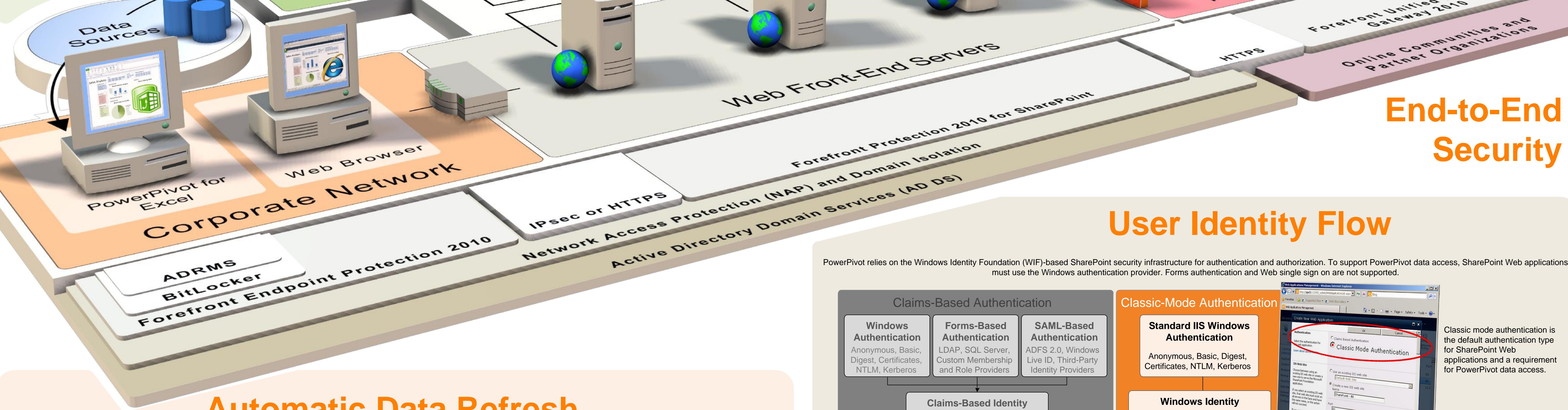
PowerPivot Application Servers



Service Account Management



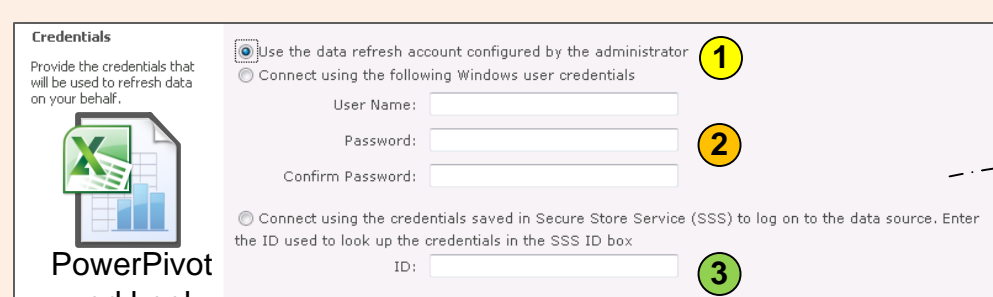
To change managed account passwords frequently, configure a password change schedule in SharePoint Central Administration or in Windows PowerShell. Password updates will not be reflected in any credentials stored in Secure Store Service.



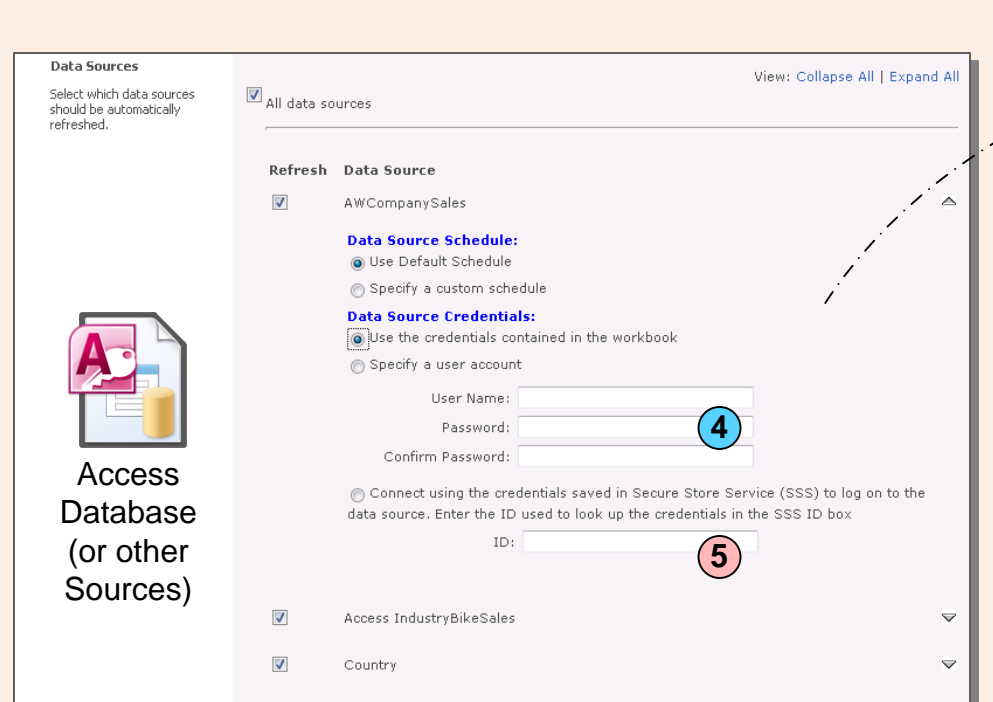
Automatic Data Refresh

Analysis Services instances can perform automatic or scheduled data refresh for PowerPivot workbooks published in a SharePoint farm if the data sources are available to the server. Unlike query databases, which are loaded in read-only mode, data refresh databases are loaded in read/write mode.

Data Refresh Credentials

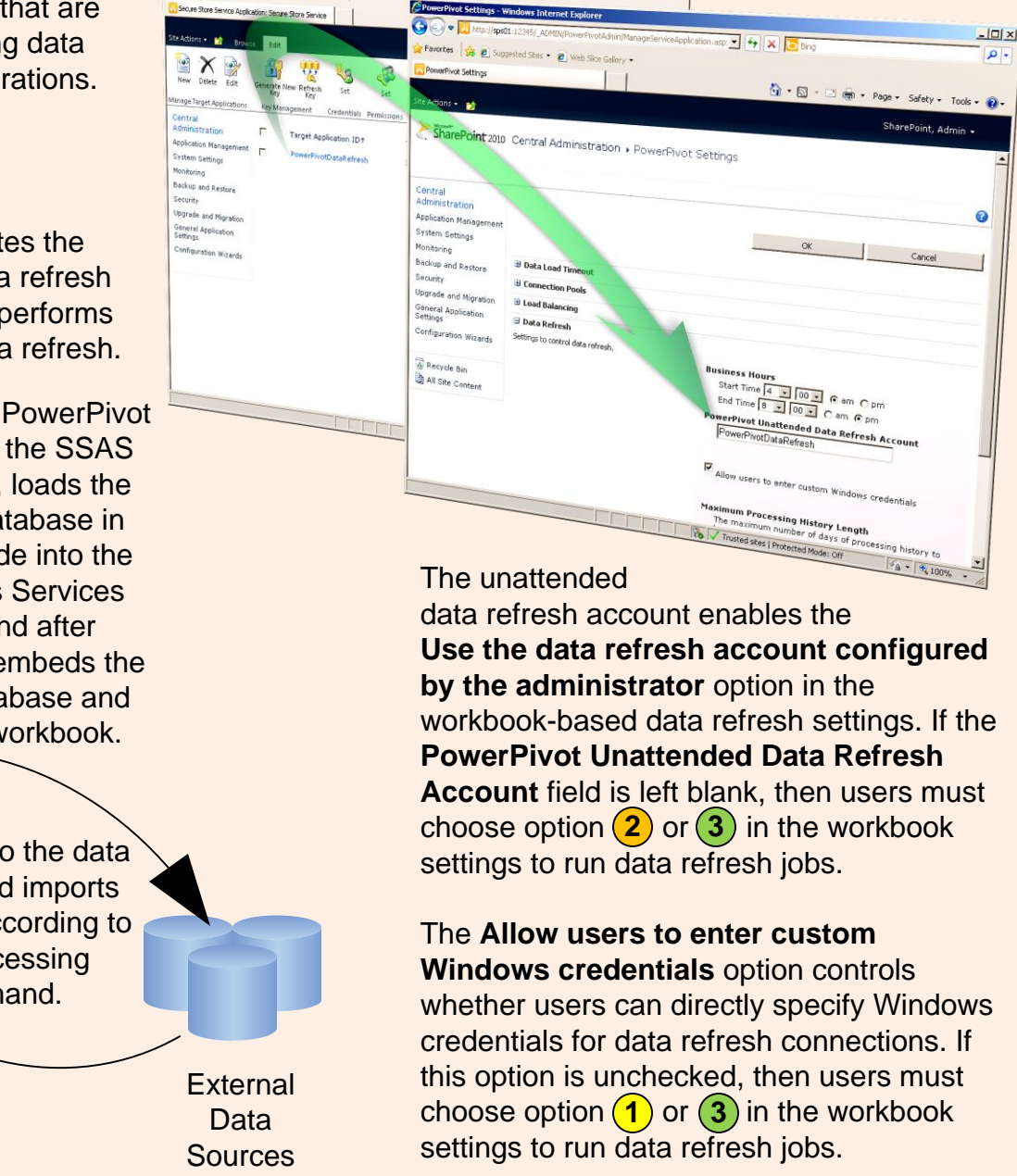


There is only one data refresh account per workbook, which must be a Windows user account with contributor (read/write) access to the workbook. This account will also be used as the Windows user identity if the workbook's data sources use trusted connections.



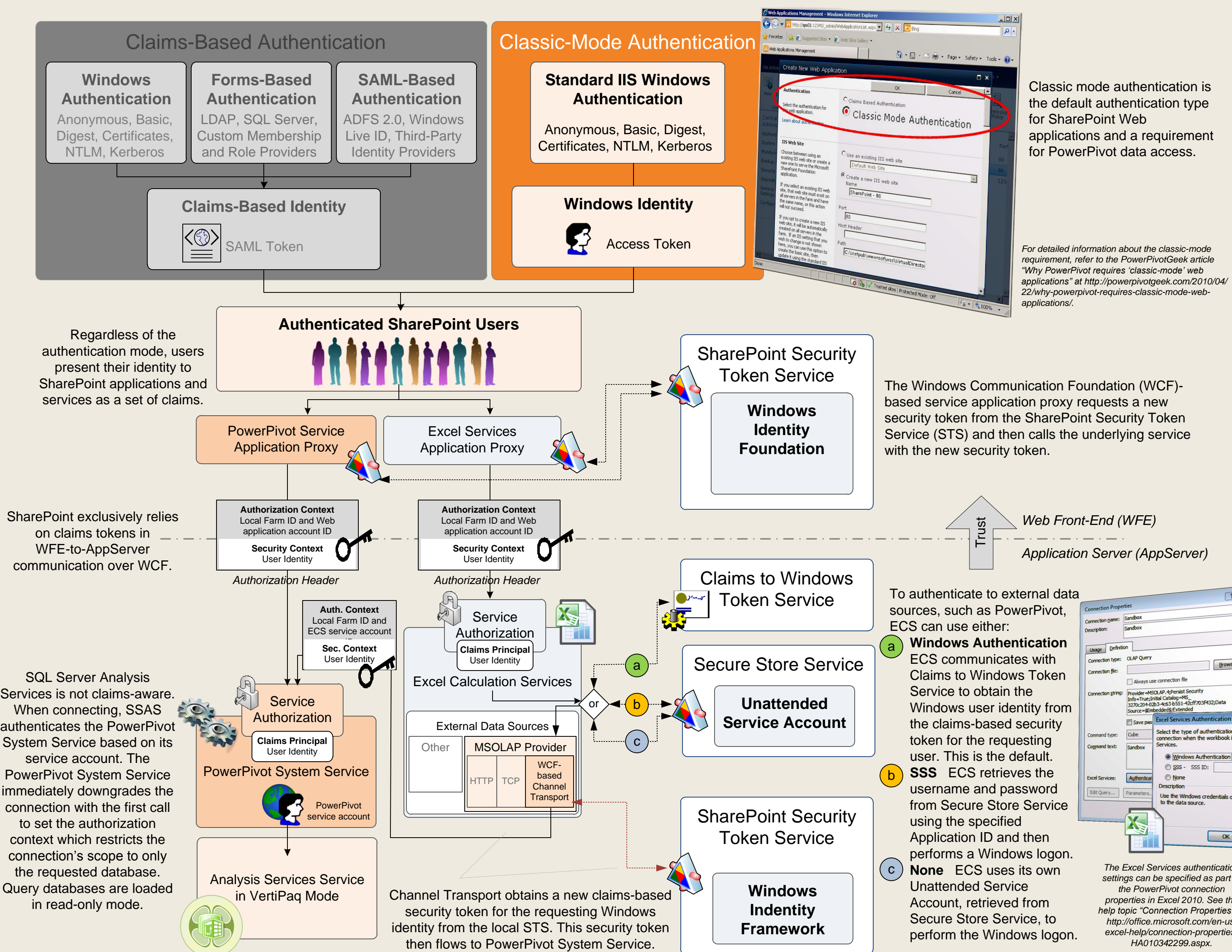
Certain data providers might have their own security configuration requirements. For example, to use the Microsoft ACE provider, the data refresh account needs to have write access to the SSAS engine's Temp folder and the Desktop Experience feature must be installed if accessing SharePoint files.

Administrative Data Refresh Settings



User Identity Flow

PowerPivot relies on the Windows Identity Foundation (WIF)-based SharePoint security infrastructure for authentication and authorization. To support PowerPivot data access, SharePoint Web applications must use the Windows authentication provider. Forms authentication and Web single sign on are not supported.



PowerPivot Permission Levels

PowerPivot takes advantage of the SharePoint security model for granular control over administrator roles and user permissions. Organizations can delegate administrative tasks at the farm, shared services, servers, and site collections levels of the administration hierarchy, and can establish separate permission levels for the producers and consumers of intelligence in each department and team.

Farm Administrators

- Install, enable, and configure Web applications, site collections, services, and other resources that pertain to the SharePoint farm.
- Deploy the application-level PowerPivot solution for individual Web applications.
- Delegate administration of service applications, including the PowerPivot service application.

PowerPivot Service Application Admins

- Manage existing PowerPivot service applications.
- Have access to PowerPivot Management Dashboard and can view administrative reports.

Analysis Services Administrators

- Local administrator access granted through WSS_WPG and SQLServer\MSASUser<server name>\\$database instance> group memberships.
- Can configure Analysis Services memory settings, backup folder path, and port numbers in SQL Server Enterprise Studio (SSMS).
- Should never use SSMS to modify server state or account information.

Site Collection Administrators

- Activate the PowerPivot feature at the site collection level.
- Manage sites, libraries, and PowerPivot galleries.
- Grant permissions to site administrators and other users.

Producers of Intelligence

- Create PowerPivot workbooks in Excel 2010.
- Contribute permissions enable upload, edit, and deletion of PowerPivot workbooks in SharePoint.
- Configure the data refresh schedule and create linked reports in PowerPivot galleries.

Consumers of Intelligence

- Work with PowerPivot workbooks by using Excel Services or Excel 2010.
- View-only permissions enable online access without downloading. Read permission, to download.
- Can use PowerPivot workbooks on a SharePoint site as data sources in local workbooks.



About PowerPivot Security Architecture Poster

Authors: Kay Unkroth

Technical Reviewers: Dave Wickert, Denny Lee, Heidi Steen, Lee Graber

Published: 08/2010

Applies to: SQL Server 2008 R2

Summary: This poster shows the PowerPivot security architecture at a detailed level to highlight how PowerPivot takes advantage of the security frameworks, encryption technologies, and policy controls available on the Microsoft business intelligence (BI) platform while providing seamless access to user-generated workbooks shared in a SharePoint farm environment.

Copyright

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft, Access, Active Directory, BitLocker, Excel, Forefront, PowerPoint, SharePoint, SQL Server, Vertipaq, Windows, Windows PowerShell, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.