VIS SHAREPOINT FOR GOVERNMENT:

AN ESSENTIAL PART OF THE IDENTITY MANAGEMENT INFRASTRUCTURE

Background:

SharePoint is a Microsoft based web application platform that offers an organization the ability to manage and share information from multiple applications in one location. SharePoint is designed to streamline workflows and increase efficiencies surrounding content and application development, document and content management, intranet and extranet functionality and enterprise-level search capabilities.

"SharePoint is a Microsoft based web application platform that offers an organization the ability to manage and share information from multiple applications in one location."

Why SharePoint for Government?

SharePoint is a Microsoft based web application platform that offers an organization the ability to manage and share information from multiple applications in one location. SharePoint is designed to streamline workflows and increase efficiencies surrounding content and application development, document and content management, intranet and extranet functionality and enterprise-level search capabilities.

SharePoint Challenges

Although SharePoint provides a good foundation for increased workflow efficiencies and collaboration, there are still several challenges when customizing the platform to integrate seamlessly with an organizations unique specifications and structure.

For example, SharePoint on its own does not have the ability to merge user information when it exists in multiple LDAP directories or AD forests. This can make it difficult for government agencies to access SharePoint when their identity data is stored in separate locations depending on the particular agency or department.

SharePoint Challenges for Federal Governments:

Out of the box, SharePoint cannot be deployed across multiple active directory forests without a trust and it is a grueling, timely process when trying to deploy access to both internal and external users. This particularly presents a challenge when a government agency is trying to share information with external agencies such as a police or fire department.

In addition, because SharePoint is such a robust platform, the administration process can be overwhelming and time consuming especially when constantly having to manage users, groups and permissions. Security and compliance can be compromised due to a lack of flexibility allowing users' access to more information than necessary and a lack of visibility due to the limited audit reporting available. These are all challenges that organizations and particularly government agencies cannot afford to face.

VIS for SharePoint

Virtual Identity Server for SharePoint is a secure, manageable multi-forest solution that provides intelligent claims-based authentication and federation in SharePoint. In other words, VIS for SharePoint enables organizations to effectively deploy and maintain SharePoint in a secure, manageable fashion, saving them time and greatly reducing total cost of administration.

Key Features of VIS for SharePoint

Below are just some of the key features that make Virtual Identity Server for SharePoint essential to getting the most value possible out of SharePoint;

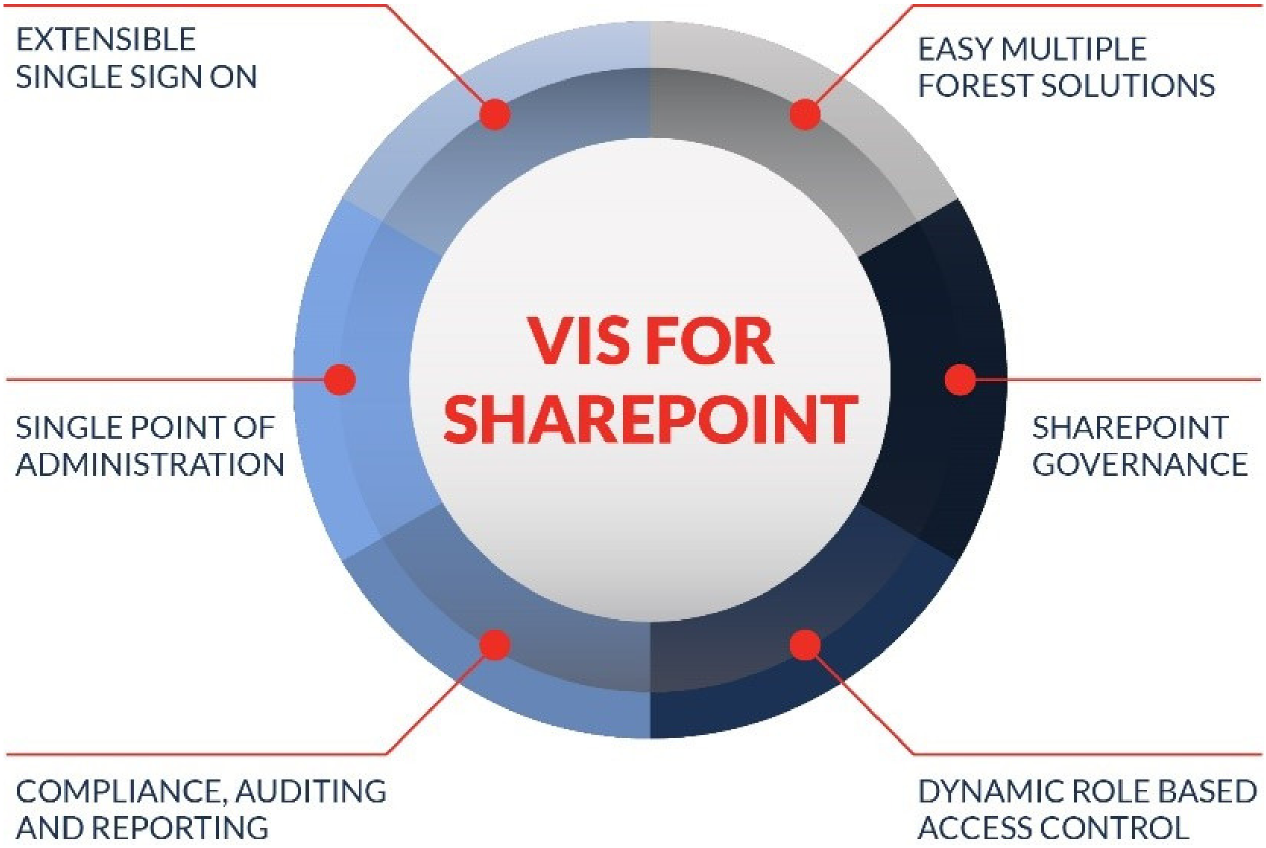
- **Virtual Static & Dynamic Groups** - enhance the security model providing a more robust, flexible solution
- **Extensive Audit & Compliance Reporting** – a complete audit and compliance solution with built-in reporting
- **Multi-Forest Solution** - Deploy SharePoint rapidly across multiple Active Directory forests without trusts
- **Two-Factor Authentications** – increased security using SecurID, Smart Card, USB Token, etc.
- **Forms Based Authentication** – can span multiple forests and multiple platforms such as Active Directory (AD) or any data store

Key Features of VIS for SharePoint (Contd.)

- **Federation** – seamless integration among systems and applications supported via our STS standalone or integrated with AD FS
- **CAC Authentication** – Department of Defense, Common Access Card (CAC) authentication
- **Digital Certificates** – Seamless login via client certificates
- **Single Sign-On** – on secure login providing seamless access to systems and applications
- **People Picker / Claims Provider** - ability to search for users/groups across all identity stores

Why VIS SharePoint for Government

Virtual Identity Server for SharePoint offers significant benefits for any organization, however, VIS for SharePoint offers specific benefits for government agencies that make it an essential part of the identity management infrastructure.


EXTENSIBLE SINGLE SIGN ON
EASY MULTIPLE FOREST SOLUTIONS
VIS FOR SHAREPOINT
SINGLE POINT OF ADMINISTRATION
SHAREPOINT GOVERNANCE
COMPLIANCE, AUDITING AND REPORTING
DYNAMIC ROLE BASED ACCESS CONTROL

Why VIS SharePoint for Government

First, the virtual dynamic group capabilities allows for security settings and permissions to be configured once and then they automatically get updated as data changes within the environment. VIS for SharePoint is also designed to access users from any data store whether that's AD, SQL database or any other data store. This means it does NOT require a domain controller or any admin privileges on a domain controller. The end result is increased security and governance while significantly reducing the cost of administration. This is crucial in the government sector for meeting audit and compliance regulations and complying with government budget restrictions.

Another major benefit of VIS for SharePoint for government agencies is the extensive and robust configuration abilities surrounding Common Access Card (CAC) authentication. Out of the box, VIS for SharePoint can authenticate to SharePoint with a Common Access Card (CAC). Any attribute off of the card can be validated against the Active Directory (AD), with the most common attribute being the EDIPI number. Even the validity of the CAC itself can be verified by checking the CRL.

In addition...

In addition to the information on the card, VIS for SharePoint can also call out to other systems to get more detailed information such security clearances, that can be sent as a role claims to SharePoint used to control access to SharePoint document libraries, lists, etc.

CAC authentication can be...

CAC authentication can be customized and configured to fit specific conditions. For example, anyone with a CAC can have access or additional conditions can be configured like requiring group membership to be checked before authorizing.

For an even higher level of security, authentication via CAC can also be configured to send a workflow request to a Del admin to approve or deny before authorizing access. Workflow requests as well as auto self-registration and account creation can significantly reduce the time and cost of administration.

VIS for SharePoint can also be configured to allow non-CAC users to access certain information on SharePoint. This is essential when government agencies need to share information with first responders such as firefighters, police or ambulances. These users can login via a user ID and password that can be stored in the VIS – there is no need to access the Active Directory. Non-CAC users can even self-register for an account and request access via a multi-level workflow approval. A similar configuration can be set up for classified and non-classified users, requiring CAC access and/or a user ID and password for either user base.