



Seclore for Microsoft SharePoint

Extending the security of Microsoft SharePoint beyond its perimeter

Documents stored within Microsoft SharePoint are often highly confidential – ranging from invoices to Intellectual Property. User specific access permissions can be defined on SharePoint libraries to mitigate security risks. However, what happens when files are checked out or downloaded from SharePoint? And then shared outside your organizational network to vendors or contractors? Or accessed on mobile devices?

Making Microsoft SharePoint Even Better

The Seclore Connector for Microsoft Sharepoint enables you to control your files even after they have been

downloaded. By securing information at the point of download, Seclore extends your security to wherever the files travel. Seclore's Enterprise Rights Management permissions can be linked to the Microsoft SharePoint library permissions for each user. This ensures a common policy framework for information inside Microsoft SharePoint as well as outside it – and provides a seamless extension of your existing data governance policies.

A pre-built Seclore ERM Connector for Microsoft SharePoint enables you to add information-centric ERM capabilities to Microsoft SharePoint quickly and seamlessly.

You can control who can access a file, what they can do with it, when, and from which computer or device. Such persistent, filecentric controls empower

you to increase the scope of Microsoft SharePoint security and governance to files travelling through public and partner networks, stored on the cloud or file-sharing services, or accessed on mobile devices.

Seclore's Enterprise Rights Management security policies allow information access for each file based on four criteria:



WHO can access the file?
User or Groups Within or Outside the Organisation



WHAT can they do with it?
View, Edit, Print, Copy Content, Take Screen Grabs, Work Offline

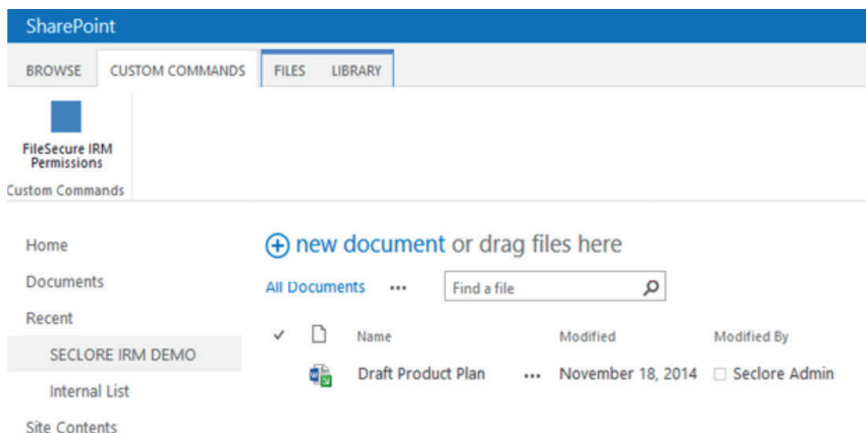


WHEN can they do it?
Automatic File Expiry, Date and Time Ranges, Number of Days from First Access



WHERE can they do it?
Specific Computers or Devices, Specific IP Address

These controls are applied on the file itself and are independent of the computer, device, network, storage, or transmission technology used. The permissions are completely dynamic: any change in the Microsoft SharePoint permissions is instantly applied to all previously downloaded files as well.



Seclore's Enterprise Rights Management policies being applied on a Microsoft SharePoint library

Key Features

Extending Security Beyond Microsoft SharePoint

Microsoft SharePoint and Seclore's Enterprise Rights Management, when combined, keep your data in your control – even when it leaves Microsoft SharePoint's control. Seclore ERM can seamlessly take over where SharePoint protection ends – and then stay with the file wherever it travels

Common Access Permissions and Policy Framework

Security policies on downloaded files can be managed from Microsoft SharePoint itself. Access permissions in downloaded files are applied directly from Microsoft SharePoint library permissions. For example, if a user's access to a library is revoked, his/her access on all previously downloaded files also gets revoked – automatically and instantly.

Audit Trails

The combined auditing capabilities of Microsoft SharePoint and Seclore ERM provide complete visibility over document usage at all times. All activities performed on protected files – whether inside or outside the enterprise network – are centrally logged. Many forensic details such as date and time, machine name, IP address, and file path are also available

Remote-Control

The file owner can control access to the information even after it has been shared. All changes in access permissions take effect in realtime

Complete Automation

The file gets protected automatically just before being downloaded – with no user intervention needed. The entire process is transparent to the end user

Seamless Workflow Integration

ERM access policies on files can be mapped to information flow and data usage patterns – without affecting business workflows.

Key Business Benefits

Increased Business Agility

You obtain the freedom to secure information that travels beyond your corporate borders – to vendors, partners, and contractors – and adopt new trends such as Cloud Computing, file sharing, BYOD, and enterprise mobility with confidence. Enabling secure collaboration makes your business more agile while significantly reducing your security risks.

End-to-End Auditing and Regulatory Compliance

You can now govern your information throughout its entire lifecycle – both within and outside your enterprise boundary.

Minimum IT Overhead

Once Microsoft SharePoint and Seclore's Enterprise Rights Management policies are configured and mapped, there is little need for any IT involvement. All changes to Microsoft SharePoint policies are automatically applied on previously protected files as well.

Increased ROI from Your Box Investment

By enabling information-centric security on stored and downloaded documents, the addition of ERM with file-sharing drives maximum value of your investment.

USA – West Coast

691 S. Milpitas
Blvd.#217
Milpitas CA 95035
1-844-473-2567

USA – East Coast

420 Lexington Avenue
Suite 300,
Graybar Building
New York City
NY 10170

India

Excom House Second Floor
Plot No. 7 & 8,
Off. Saki Vihar Road
Sakinaka, Mumbai
400 072

+91 22 6130 4200
+91 22 6143 4800

Gurugram

+91 124 475 0600

Singapore

Seclore Asia Pte. Ltd.
AXA Tower, 8 Shenton
Way
Level 34-01
Singapore – 068811

+65 8292 1930
+65 9180 2700

Europe

Seclore GmbH
Marie-Curie-Straße 8
D-79539 Lörrach
Germany
+49 151 1918 5673

UAE

Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City, PO Box
73030, Dubai, UAE
+9714-440-1348
+97150-909-5650
+97155-792-3262

Saudi Arabia

5th Floor, Altamyo Tower
Olaya Street
P.O. Box. 8374
Riyadh 11482
+966-11-212-1346
+966-504-339-765

