Workshare Compare in NetDocuments

Data Security

July 2019

Table of Contents

Overview

This document explains the data security measures in place for Workshare Compare in NetDocuments.

It covers data in transit as it is transferred to and data at rest within the *Workshare Compare Service*.

Introducing Workshare Compare in NetDocuments

Workshare Compare in NetDocuments is an integration between the Workshare Compare Service and NetDocuments, in which users can select two documents that reside in their NetDocuments repository, and compare them in the browser using Workshare's hosted comparison application.

Workshare's Compare Service is hosted in Azure, in three regions – US, EU, AU, and is owned and operated by Workshare.

The integration, Compare in NetDocuments, is thus available in the three available NetDocuments regions – US, EU, and AU.

Our approach to security

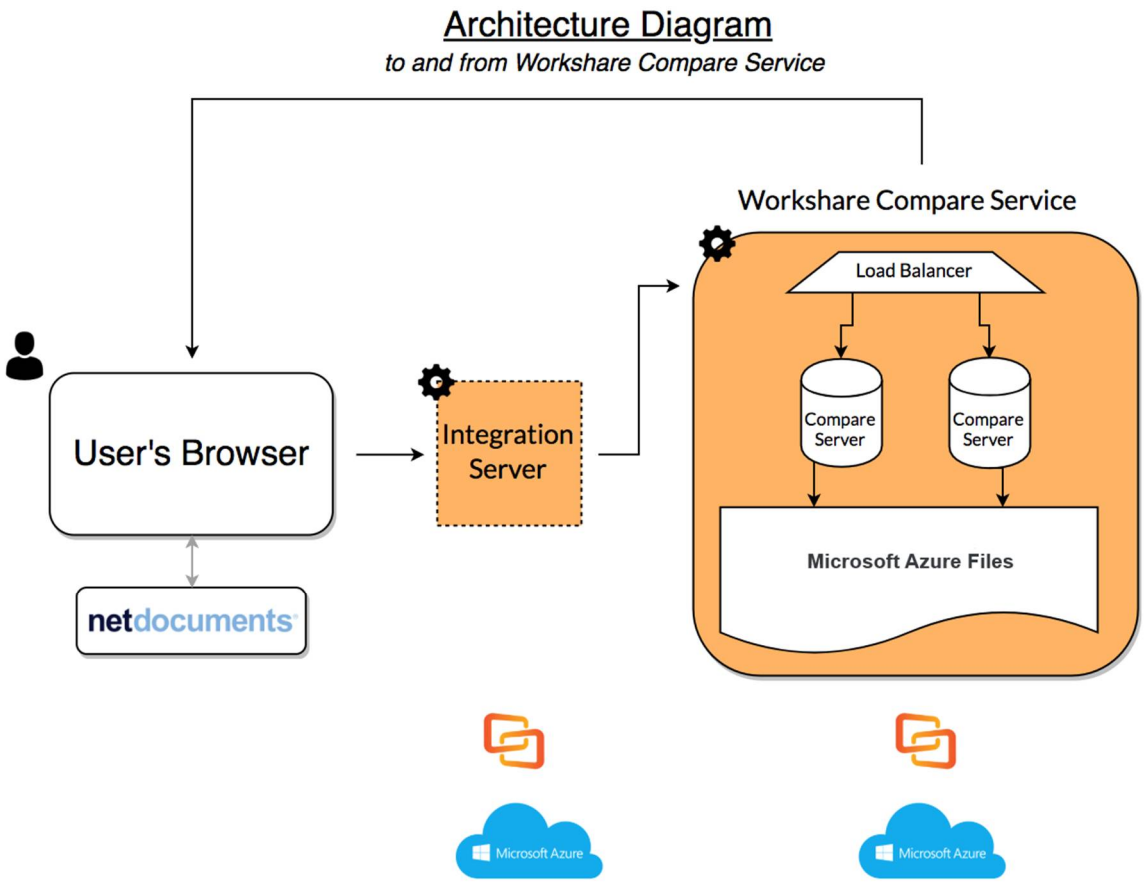
Workshare has obtained the ISO 27001:2013 certification in respect of information security.

We know that keeping customer data safe and secure is of paramount importance and one of our most important responsibilities.

We are dedicated to ensuring that our customers have the highest confidence in our security practices and infrastructure.

System Architecture

The following diagram shows the architecture of the system as a whole.



Data Security: How data is secured between NetDocuments and the Compare Service

User Actions

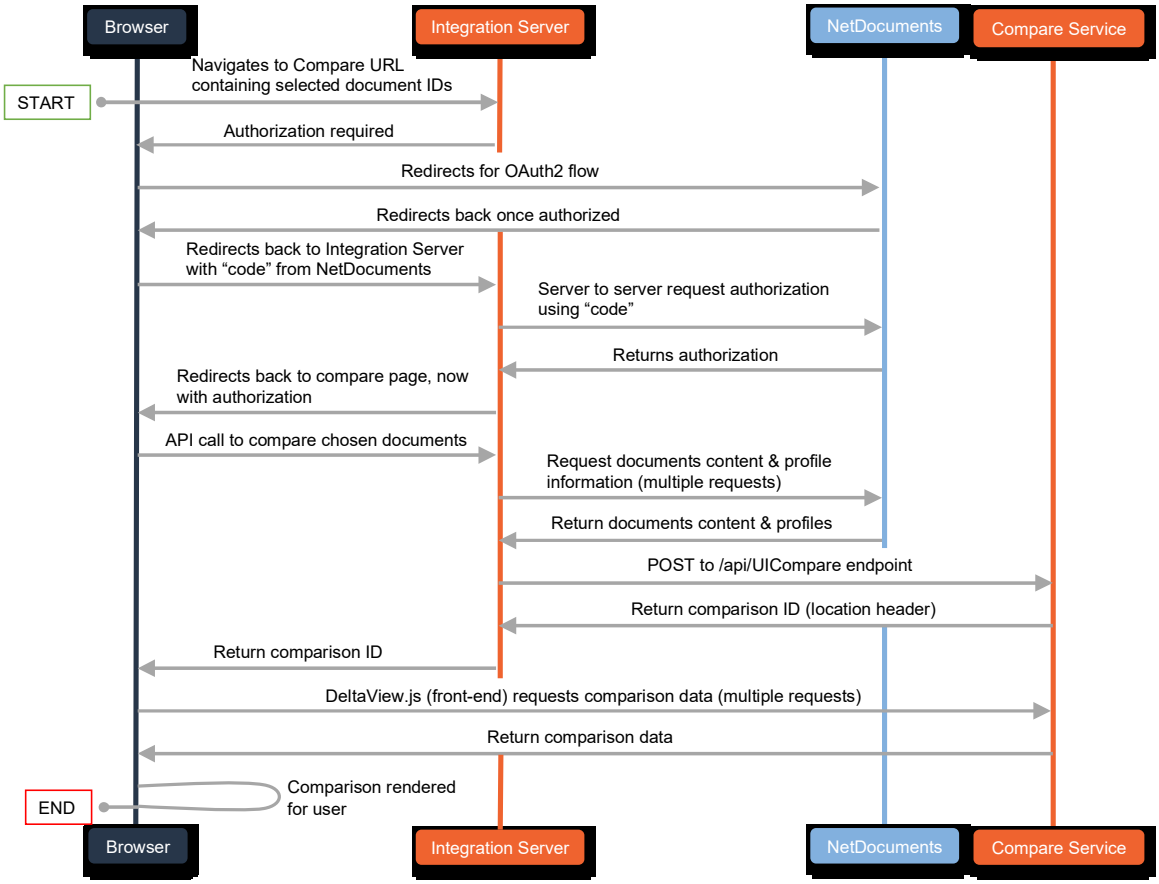
The following diagram shows the flow of data when:

1. Two documents are selected in NetDocuments
2. NetDocuments' 'Send To Application' function is launched
3. Comparison is run

4. Comparison is displayed within NetDocuments, in the Workshare Compare online interface.

System Actions

To achieve the above, the following system actions take place. The data flow is initiated in the user's browser and flows through the various components of the Workshare Compare Service ecosystem.



All calls shown above are made using HTTPS and therefore all communication is encrypted

How data is secured by the Workshare Compare Service

The following explains how data at rest is treated in the Workshare Compare Service ecosystem.

- Request for comparison arrives (with the source documents) and Compare Server generates a Comparison ID.
- The Comparison ID is unique to each comparison. It is a cryptographically secure random token with 192 bits of entropy.
- Compare Server encrypts the source documents using a key generated from the Comparison ID.
- The encrypted source documents are stored in Microsoft Azure Files.
- Compare Server decrypts the source documents using the Comparison ID and runs a comparison.
- The source documents are temporarily written to local disk while they are being pre-processed for comparison or while being post-processed after comparison. These temporary documents are automatically deleted as soon as the comparison has completed.
- The results (UI compare resources) and the source documents are encrypted using the Comparison ID and stored in Azure Files.
- When the user requests to view the comparison, Compare Server decrypts the results using the Comparison ID and sends them via HTTPS back to the user's browser.
- Documents may be temporarily written to local disk while they are being pre-processed for comparison or while being post-processed after comparison. These temporary documents are automatically deleted as soon as the comparison has completed.
- One hour after the comparison is performed, a scheduled task tells Microsoft Azure Files to expunge (delete) the source documents and the results (UI compare resources). If this fails for any reason, Azure Files will auto purge after 24 hours.

***Note**: Data is not stored in the Integration Server.*

What does Microsoft Azure Files offer in the way of security?

The key features of Microsoft Azure Files security are automatically applied by default within our Compare Service allowing us to prevent, detect, and respond to breaches. In particular, Azure Files:

- Encrypts data at rest. For more information, see Azure Storage Service Encryption.
- Provides access restrictions at the storage account level so we can restrict access by IP and user credentials. For more information, see Configure Azure Storage Firewalls and Virtual Networks.

For more information about Microsoft Azure Files security, see the Azure Storage Security Guide.

Microsoft Azure

The Workshare Compare Service runs in Microsoft Azure. The Compare Servers that live within the Compare Service infrastructure do not have public IP addresses, and thus are not directly exposed to the internet. The servers only accept HTTPS traffic from the Azure Load Balancer – no other in-bound traffic is allowed.

The servers also make use of encryption-at-rest (AES-256 for any data that they hold (as per the example in 3.0 above).

The following article describes the various security measure Azure has in place as a platform. https://docs.microsoft.com/en-us/azure/security/

Penetration Testing

Penetration testing on the Workshare Compare Service is owned by Workshare, and carried out by Pen Test Partners, every 4 months from April 2019 onwards.

Organizational Security

Introduction to ISO 27001

Workshare has obtained the ISO 27001:2013 certification in respect of information security. The ISO certification is renewed annually and requires that organizations adopt information security policies across a number of areas of the business.

Our certificate is available here:

https://www.workshare.com/governance-and-security/information-security/iso-27001-certificate

Policies and standards

We maintain a set of policies that set out our procedures and practices for ensuring compliance with our information security obligations and requirements.

The policies that we have adopted in compliance with the relevant ISO standards include the following:

- Information security policy
- Organization of information security
- Human resources security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

Personnel security & screening

Our personnel practices apply to all members of the workforce (regular employees and independent contractors) who have direct access to our internal information systems. All workers are required to understand and follow internal policies and standards.

Before gaining initial access to systems, all workers must agree to confidentiality terms and attend security training. This training covers privacy and security topics, including device security, acceptable use, preventing malware, physical security, data privacy, account management, and incident reporting.

Security responsibilities

We have defined roles and responsibilities to determine responsibility for operating the various aspects of our product security and information security program, as follows:

Product security

- Build and operate security-critical infrastructure including public key infrastructure, event monitoring, and authentication services
- Establishing secure development practices and standards
- Ensuring secure coding practices
- Reviewing code for detection and removal of security issues
- Ensuring regular penetration testing and implementing recommendations
- Manage vulnerability scanning and remediation
- Maintain a secure archive of security-relevant logs

Information security

- Develop and maintain relevant information security policies
- Monitor compliance with applicable data legislation
- Manage and maintain compliance with ISO:27001 certification
- Coordinate regular risk assessments
- Manage the security awareness program
- Respond to customer inquiries

Security incidents and response

We have established policies and procedures for responding to potential security incidents. All incidents are managed by our Incident Response Team (**IRT**) from the point of identification of the potential incident. The IRT is headed by the CFO.

Our incident response policy defines the types of events that must be managed via the incident response process, and sets out steps to be taken, dependent upon the severity of the relevant incident.

Our policies provide for the notification to customers of the discovery of any unauthorized use or disclosure of confidential information or personal information by Workshare or any relevant third parties.

Physical security

CCTV monitoring is in place at all Workshare offices where employees have access to the Workshare Connect application and non-employees accessing Workshare offices are recorded and issued with visitor permits.