جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

INFORMATION TECHNOLOGY DEPARTMENT

IT Backup Services

CLASSIFICATION – PUBLIC

Policies & Procedures

Druva inSync Endpoint Backup Access Procedure

Last Updated :	**March 9,2017**
Version :	**2.0.0**
Document :	**Druva_inSync_Endpoint_Backup_Access_Procedure.2.0.0.docx**

جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

Version Control

Document Version	Revision	Date	Author(s)	Change Reference
Draft 1	Draft	January 7, 2015	Ronald M. Serato	Draft
Draft 2	Draft	January 22, 2015	Ausaf M. Rasheedi	Draft
1.0.0	Final	February 22, 2015	Ronald M. Serato, Ausaf M. Rasheedi	Initial Release
2.0.0	Final	March 9, 2017	Omar A. Alattas	Disable mobile device backup

جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

Contents

1. Introduction

1.1 Purpose

Druva inSync is a backup solution for end-user's Windows, Mac and Linux clients.

The solution allows eligible end-users to protect their endpoint devices (laptops/desktops) by having an inSync client running on them. The objective is to protect business data in these devices from any data loss, by manually selecting the critical and important folders that end-users choose to backup.

1.2 Scope

This document highlights the access procedure to the inSync and eligibility of user access to this application.

2. Product Information

inSync application comprises of two components:

- inSync On premise Server
- inSync Client

3. inSync Security Architecture

inSync authentication is achieved securely through MS Active directory (AD). The eligible end-users and administrators gain access to the service after their AD accounts are imported to the inSync servers. Subsequently, end-users devices have to be registered with the inSync servers before the service becomes fully available to them. If the end-user AD account is disabled by the IT Windows team, the end-user access gets disabled on the respective inSync node.

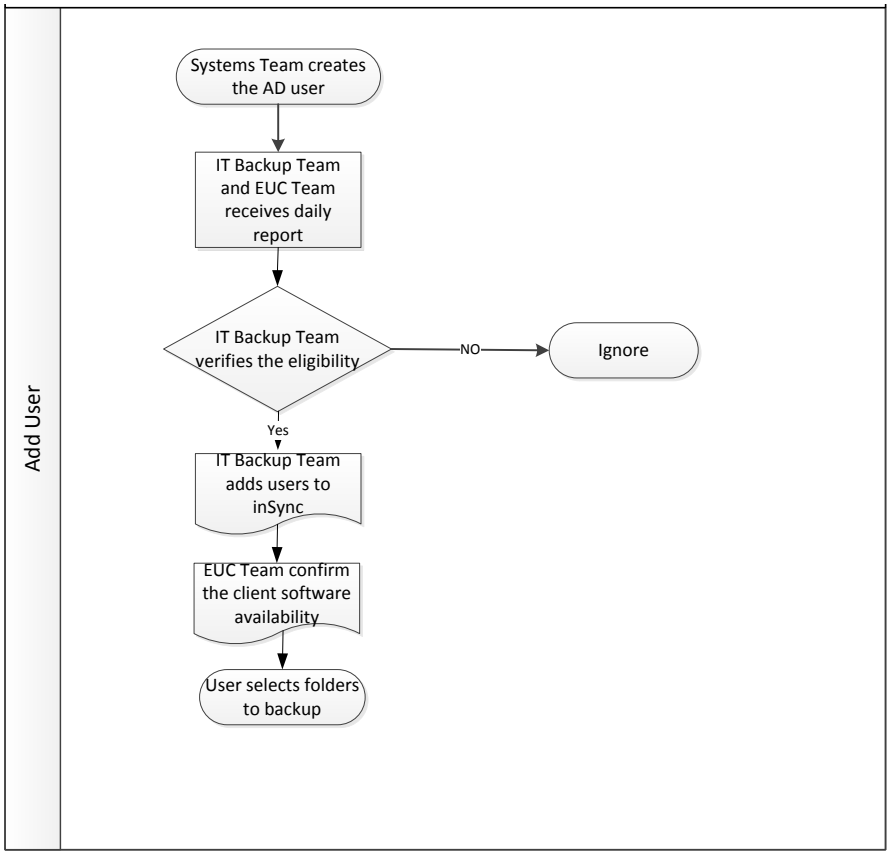
User data on the inSync nodes is completely secured and private i.e., by default, the admin view or download of the user data is disabled.

4. Scope and Eligibility

This solution is only available to Faculty and Staff (including the Consultants and STEC) With AD credentials and a valid KAUST e-mail address due to its integration with active directory. Some exceptions may apply based on business justification and approvals.

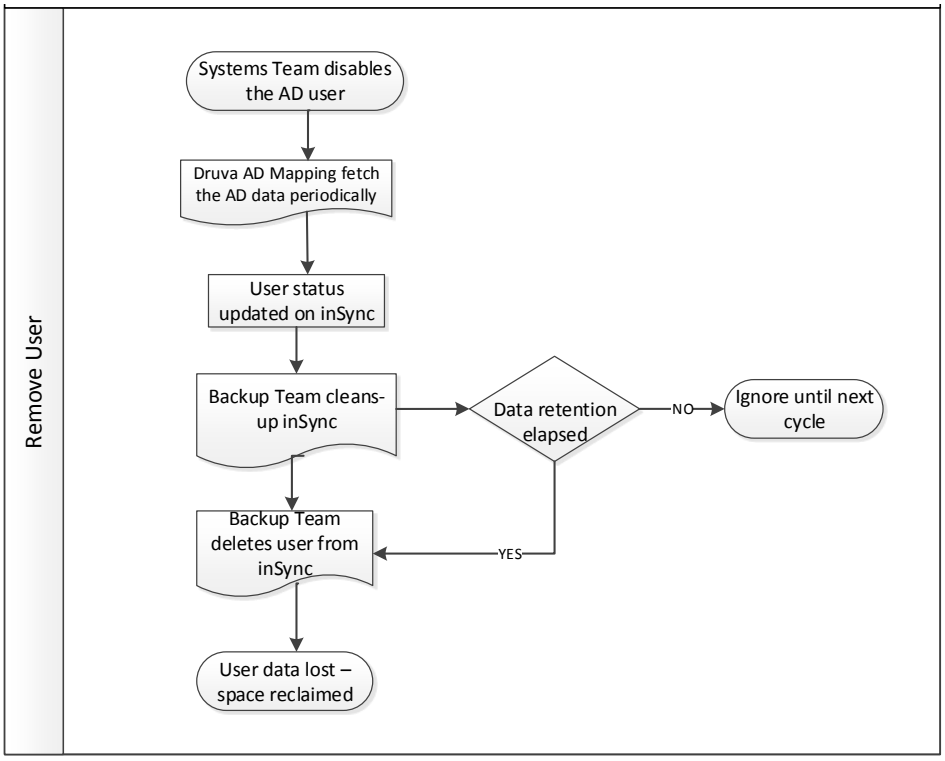
5. Access Procedure

- A new hire's Active Directory (AD) user account is created on the Active Directory server.
- An automated report is sent out daily with information regarding users provisioned.
- IT Backup team verifies the eligibility and adds user to the inSync server.
- The newly added user receives a notification of the service availability.
- EUC installs the client if required. The druva insync client is part of the Operating system (OS) image, prepared by the EUC team.
- End-user activates device and chooses the folder(s) required for backup.



6. Removal Procedure

- The Druva server is using Active Directory (AD) mapping feature of Druva application that pulls data for existing users from Active Directory periodically.
- IT Windows team disables the user on AD; it is fetched by Druva and subsequently disabled users are disabled on Druva application. The frequency of auto-updating existing users from AD is set to every 8 hours.
- The disabled users' data is retained on the Druva server until retention is expired.
- IT Backup team carries-out the clean-up process on the Druva server on a monthly basis, and deletes all the users from Druva server that are disabled 2 month ago.
- Deletion of the user from the Druva server subsequently deletes the user data and devices from the server, and as a result storage space is reclaimed.



7. Data Retention

End-user's backup data is retained for a maximum of 3 months.

8. Inactive Devices

The user receives an email notification, after two weeks of inactivity or device(s) not being backed up. On completion of 3 months of inactivity, the user receives an email notification stating, that, “your account has been disabled and data will be deleted after one month”, the admin disables devices with inactive backup after three months and deletes the data post one month.

9. Business Process Procedure

- Each eligible end-user can back up a maximum of up to two devices.
- End-user has the autonomy to choose the folders to backup with the ability to access and restore on their own using inSync client or through an encrypted URL, which can be accessed from any browser.
- A snapshot of a successful back up is stored on the inSync nodes and retained for a given period of time.
- Druva is maintained and administered according to the standard operation procedures including Data backup policies and System security.

10. Support Contact

For any related queries, please contact IT helpdesk ithelpdesk@kaust.edu.sa.

11. Forms and Records

None

12. Attachments

None

13. Related Documents

None

14. References

None

جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

Proposed By

Mohamed H. Abdel-Aal

Manager, Research & Computing Infrastructure

.....

Date ..... March 19, 2017 .....

Concurred By

Larry G. Fayad

IT Services Manager

.....

Date ..... March 19, 2017 .....

Approved By

John E. Larson

Chief Information Officer

.....

Date ..... March 19, 2017