

LUWARE STRATUS RECORDING

Technical Whitepaper

Version 1.0

05 March 2020

1 REVISION HISTORY

Version	Status	Date	Author	Change Reason
1.0	First Release	05/03/2020	Mehmet Kocak	Document Creation
1.0	First Release	05/03/2020	Alexander Grafetsberger	Internal Review
1.1	Partner Preview	06/03/2020	Russell Mirams	Partner Preview prior to final release
1.2	Addition	09/03/2020	Mehmet Kocak	Replace placeholder diagram

2 APPROVERS

Name	Organization	Position and Role	Version Approved
Alexander Grafetsberger	Luware UK Ltd	Executive Director, Product Manager	1.0

Contents

1 Revision History	2
2 Approvers	2
3 About this document	4
4 Target Audience	4
5 Luware Stratus Recording Overview.....	5
6 Recording Capabilities.....	6
6.1 Native Microsoft Teams Recording	6
6.2 Luware Stratus Agent / STratus Team Recording.....	7
7 Customer Pre-Requisites.....	8
8 User Provisioning.....	9
8.1 Microsoft Azure AD Synchronization	9
8.2 User Synchronization Filtering Criteria.....	10
8.3 CSV Import	10
8.4 Group Synchronization Filtering Criteria:	11
9 Role Based Access Control	12
9.1 Recorded User Permissions.....	12
9.2 Supervisor Permissions	12
9.3 Admin Permissions.....	12
10 Conversation Retention Settings.....	12
11 Microsoft Teams Compliance Policies	13
11.1 Create Microsoft Teams Compliance Policies.....	13
11.2 Scripted Creation of Compliance Policies	14
11.3 Manual creation of Compliance Policies	15
11.4 White Listing Luware Stratus Recording Application	15
11.4.1 Creating Microsoft Teams Compliance Policy.....	16
11.4.2 Consent Permissions to Luware Stratus Recording Bot	17
11.5 Granting Compliance Policies to Users.....	17
12 Accessing Luware Stratus Recording Portal.....	17
12.1 Return this document.....	18
13 Appendix	19

3 ABOUT THIS DOCUMENT

This document provides guidance for a customer to enable Microsoft Teams Recording offered as a hosted service by Luware Stratus Recording.

Please be aware that at the time of writing this service is still under an Early adopter program pending final release of the associated API's by Microsoft, Verint and any adaptations by Luware to the Stratus SaaS platform and is therefore an evolving service, with specifications subject to change in future.

This document will be maintained based on any future specification changes that pertain to the sections in this document, (i.e. Feature and Functionality improvements, Microsoft Teams Compliance Recording PowerShell CMDLets..)

4 TARGET AUDIENCE

This is mainly targeted at a Technical Audience who should be familiar with Microsoft Teams, PowerShell and O365 Services in general.

5 LUWARE STRATUS RECORDING OVERVIEW

Luware Stratus Recording is a cloud hosted solution that customers can integrate with from their existing Microsoft Azure and Microsoft Teams estate for the purpose of recording conversations.

Luware Stratus Recording is available for customers consuming Luware Stratus Agent and or Team for their Microsoft teams contact centre agents as well as for customers purely wanting to recording standalone Microsoft Teams users. Stratus Recording is a Luware Cloud offering intended to be provided as a 24/7/365 service subject to scheduled and announcement maintenance windows.

Recording capabilities are described further on in this document however there are two logical platform recording concepts:

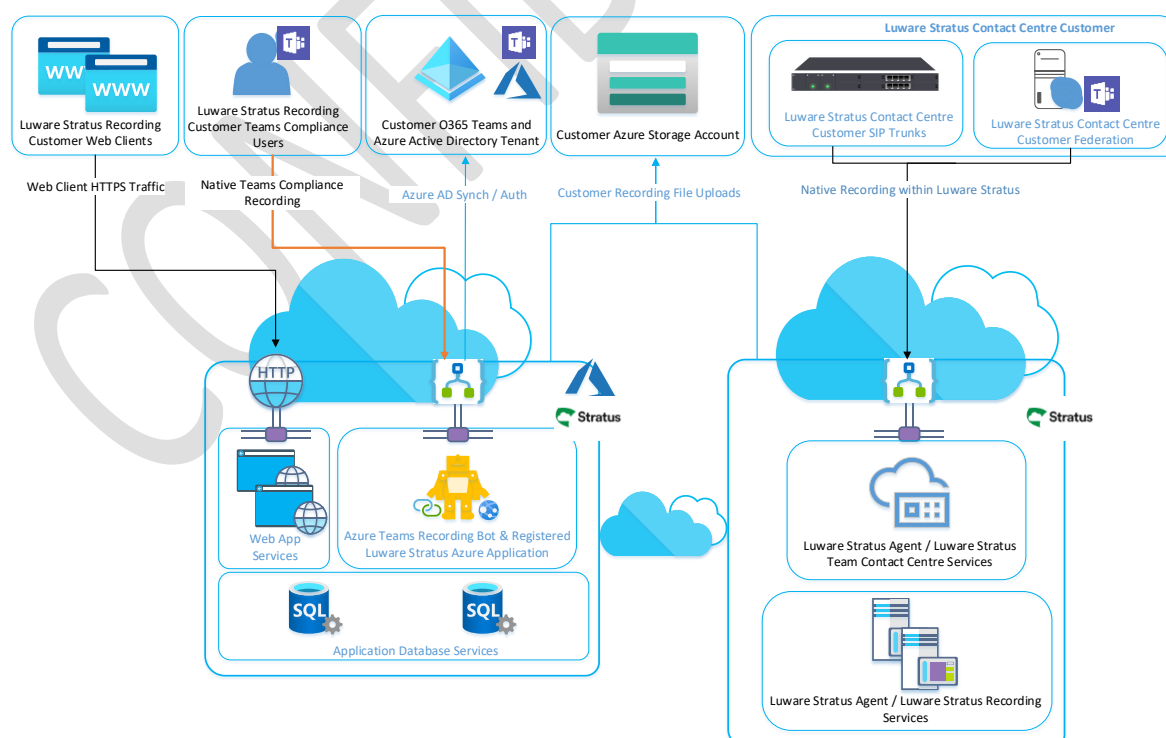
- Recording for Microsoft Teams native conversations
- Recording for Luware Stratus Agent and or Team Contact Centre conversations

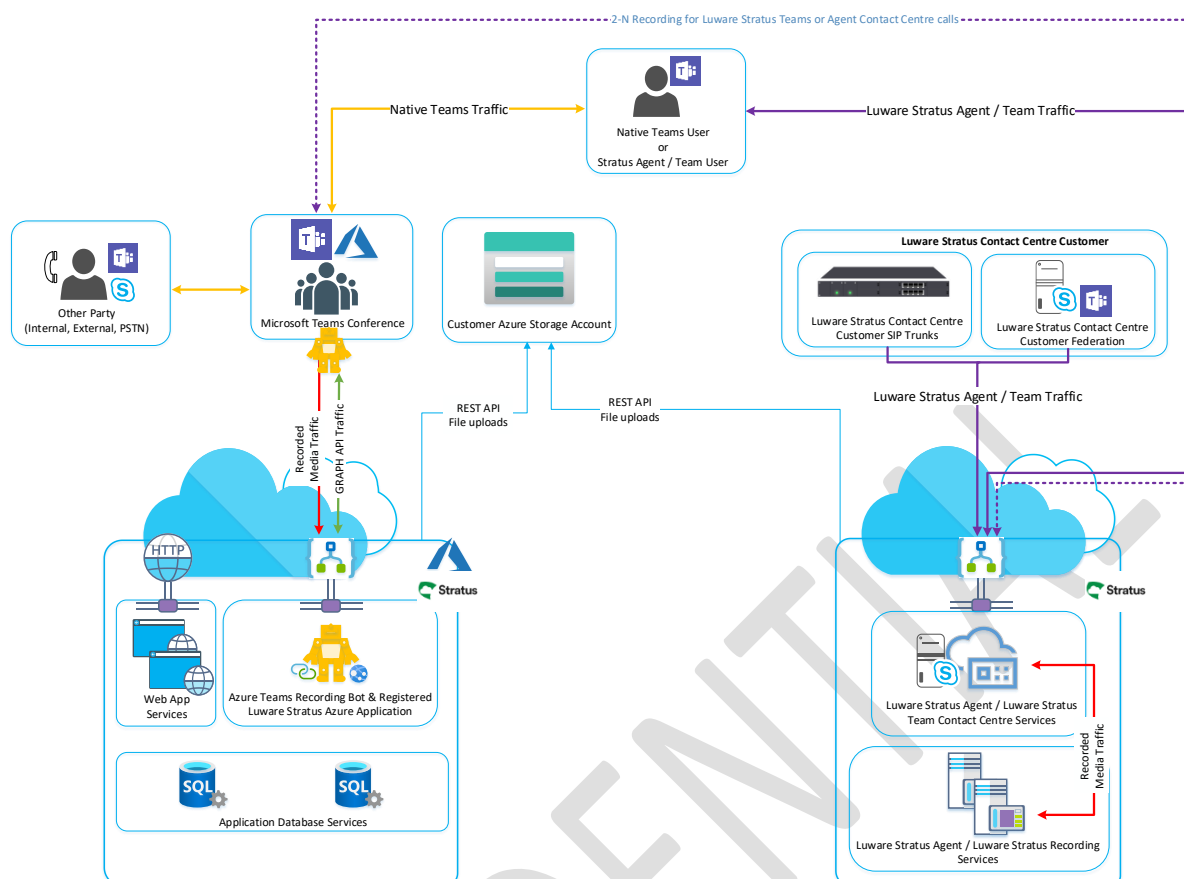
These can be configured for customers who are simply capturing for internal purposes using the basic license, or for Compliance grade retention using the Advanced Licensing, as defined in the Solution Description documentation.

At the time of initial release, the primary platform components for Luware Stratus Recording for native Microsoft Teams is hosted within Microsoft Azure, specifically within the North Switzerland Region of the Azure platform. However MS Teams users from any Teams location worldwide can be captured in real-time.

The primary platform components for Luware Stratus Recording for Luware Stratus Agent and/or Team is hosted within Luware Datacentres, specifically in Zurich, Switzerland.

The customer's 'data at rest' is stored to a customer supplied Azure data store.





6 RECORDING CAPABILITIES

This section provides an overview of the recording capabilities supported today within Luware Stratus Recording hosted offering.

For a fuller description of functionality and features please see the [Luware Stratus Recording Service Description](#).

6.1 NATIVE MICROSOFT TEAMS RECORDING

Luware Stratus Recording capabilities for native Microsoft Teams conversations is detailed below, please note this as this is a beta evolving service, the specifications detailed in this section are subject to change.

Native Teams Recording Capabilities (Early Adopter):

Call Type	Modality	Availability
Internal P2P	Audio	Yes
Internal P2P	Video /Screen Share	Yes
Internal Conference	Audio	Yes
Internal Conference	Video /Screen Share	Yes
PSTN (Direct Routing or Calling Plans)	Audio	Yes
Federated P2P	Audio	Yes
Federated P2P	Video /Screen Share	Yes
Federated Conference	Audio	Yes
Federated Conference	Video /Screen Share	Yes
All**	Chat/IM**	NO**

***Chat recording: "Beta release with limitations targeted for end of March 2020, GA release targeted end of July 2020"*

Native Teams Recording Announcement Capabilities (Early Adopter):

Call Type / Direction	Announcement Type	Can be enabled /disabled	Text/Audio can be Modified
Internal P2P	Banner / Text	Yes	No
Conference (All)	Banner / Text	Yes	No
Federated/PSTN In (P2P)	Banner / Text & Audio	Yes	No
Federated/PSTN Out (P2P)	Banner / Text & Audio	Yes	No

Native Teams Recording known limitations (Early Adopter):

- Chat Recording NOT Available at the time of writing **.
- Cannot modify Announcement prompt audio or text

6.2 LUWARE STRATUS AGENT / STRATUS TEAM RECORDING

Luware Stratus Recording capabilities for Luware Stratus Agent and/or Team Contact Centre conversations is detailed in this section.

Please note that for every native Microsoft Teams recorded user that is also a contact Centre agent for Luware Stratus Agent and/or Team will have two recordings per contact Centre call handled by the recorded agent (2-n) – This cannot be disabled.

Please note the Announcement settings applied to Teams Recorded users explained in section 6.1 is not mutually exclusive and cannot be disabled for contact Centre Calls.

If a Recorded Microsoft Teams user is enabled for announcements and is also a Luware Stratus Agent and/or Team member then any Contact Centre calls handled by this particular agent will observe audio announcement played to the caller.

- **Recording capabilities (Early Adopter):**

Call Type	Modality	Availability
Federated Contact Centre IN	Audio	Yes
Federated Contact Centre IN	Video /Screen Share	Yes
Federated Contact Centre OUT	Audio	Yes
Federated Contact Centre OUT	Video /Screen Share	Yes
Federated Contact Centre IN	IM	No*
Federated Contact Centre OUT	IM	No*
PSTN Contact Centre IN	Audio	Yes
PSTN Contact Centre IN	Video /Screen Share	Yes
PSTN Contact Centre OUT	Audio	Yes
PSTN Contact Centre OUT	Video /Screen Share	Yes

** see s6.1 for comments on Instant Messaging recording

7 CUSTOMER PRE-REQUISITES

This section provide the customer a list of pre-requisites that need to be adhered to in order to be able to consume the Luware Stratus Recording hosted service.

Each of these pre-requisites is detailed further on in this document however this section is intended to provide the reader a holistic view of what needs to be performed within the customers Azure Tenant:

- I. Customer is required to create a minimum of three Azure AD Security Groups with members, these are specifically for:
 - Recorded Users
 - Supervisors
 - Admins

Please [Microsoft Azure AD Synchronization](#) for further information

- II. Customer is required to create Azure File Share Storage (this information is provided in an accompanying document: Luware Stratus Recording Azure Storage.pdf)
 - Optionally customer can also provide a cert bundle (Bring Your Own Key) to securely sign and encrypt the data stored on the customers Azure File Share Storage.
- III. Customer is required to whitelist the Luware Stratus Recording Bot Application: Please see [Microsoft Teams Compliance Policies](#) for further information
- IV. Customer is required to create Teams Compliance Recording Policies for the customers recorded users using the whitelisted application
Please see [Microsoft Teams Compliance Policies](#) for further information
- V. Customer is required to consent permissions to the Luware Stratus Recording Bot application. The permissions required by the application are detailed below – these permissions allow for Teams call recording, Azure synchronization, and Azure AD Authentication: Please see [Consent Permissions to Luware Stratus Recording Bot](#) for further information

Type	API / Permissions	Description
Delegated	User.Read	Sign in and read user profile
Application	Calls.Access.Media.All	Access media streams in a call as an app
Application	Calls.Initiate.All	Initiate outgoing 1 to 1 calls from the app
Application	Calls.InitiateGroupCall.All	Initiate outgoing group calls from the app
Application	Calls.JoinGroupCall.All	Join group calls and meetings as an app
Application	Calls.JoinGroupCallAsGuest.All	Join group calls and meetings as a guest
Application	Directory.ReadAll	Read directory data
Application	Group.Read.All	Read all groups
Application	OnlineMeetings.Read.All	Read online meeting details
Application	OnlineMeetings.ReadWrite.All	Read and create online meetings
Application	User.Read.All	Read all users' full profiles
Application	User.ReadWrite.All	Read and write all users' full profiles

- VI. Customer is required to grant the Teams Call recording policies to the desired named mandated Teams Compliance users. Please see [Granting Compliance Policies to Users](#) for further information

8 USER PROVISIONING

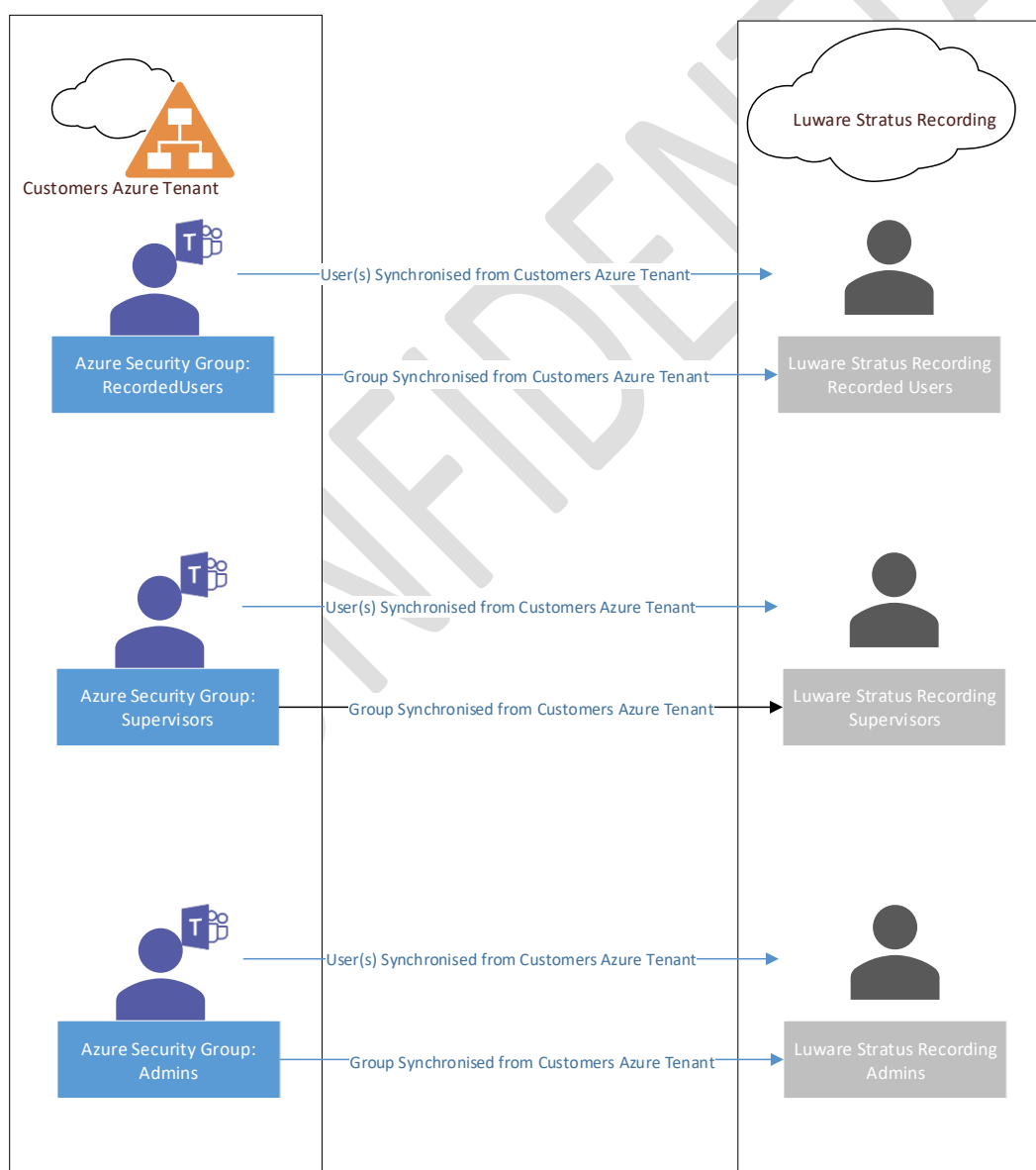
In order to onboard users (recorded users, supervisors, administrators) onto the Stratus Recording platform, the provisioning methods outlined in this chapter are available.

8.1 MICROSOFT AZURE AD SYNCHRONIZATION

This section provides the default approach for Luware Stratus Recording for user and group synchronization, from the customers Azure tenant into the Luware Stratus Recording hosted solution.

There are some points that needs to be agreed upon prior to implementation of Azure AD User and Group Synchronization, which is detailed below.

There are default “user groupings” as per standard offering, which are deployed within Luware Stratus Recording. The illustration below describes the three “groups” of Users that are expected to be synchronized into Luware Stratus Recording, from the customers Azure AD Tenant. Luware Stratus Recording performs synch operations once a day at 02:00am UTC



8.2 USER SYNCHRONIZATION FILTERING CRITERIA

In order for Luware Stratus Recording to be able to Synchronize User accounts from the customer Azure AD tenant, a filtering criterion for the three groups of users must be agreed upon.

Luware Stratus Recording will perform queries to the customers Azure Tenant in order to retrieve and synchronize Azure AD User Objects into the Luware Stratus Recording.

This is performed via Graph API calls, which uses a filtering criterion based on a subset of Azure AD User attribute(s) value only. i.e. ObjectID, UPN, DisplayName, Department, City etc..

Please enter in the table below the Attribute Name and the value for each of the three user types that Luware Stratus Recording will need to synchronize (Recorded, Supervisor, Admin):

Azure AD User Attribute Name	Attribute Value	User Type
		Recorded
		Supervisor
		Admin

For example, each group of users with the attribute "Department" with the value "RecordedUsers", "Supervisors" or "Admins" will be synced to Luware Stratus Recording with their respective settings and permissions.

Azure AD User Attribute Name	Attribute Value
Department	Recordedusers
Department	Supervisors
Department	Admins

At the time of writing only Specific Azure AD User attributes can be used, synchronizing members from Azure AD Security Groups as user objects is still under development.

8.3 CSV IMPORT

Please note if Azure AD Synchronization is not an option for the customer, a CSV import method of onboarding Users and Groups to Luware Stratus Recording can be leveraged, further information can be provided upon request.

8.4 GROUP SYNCHRONIZATION FILTERING CRITERIA:

Luware Stratus Recording will also synchronize Azure AD Security Groups from the customer Azure AD Tenant. Azure AD Group synchronization is also performed via Graph API Calls for specific Azure AD Security Group Object ID(s).

Luware Stratus Recording Groups are required and used for when configuring Supervisor conversation access filtering, and other policies implemented within the customer tenant of Luware Stratus Recording.

The customer will need to create three Azure AD Security Groups with the correct respective Group membership that aligns to the three types of users being synchronized detailed Section 8.1.

Three Luware Stratus Group Objects will be created on the first synchronization, initial and subsequent synchronization jobs will maintain the Luware Stratus Group membership for users that are also synchronized (detailed in section 8.1). Please note that the customer must ensure that the Azure AD Security Group Membership are maintained correctly.

For each Azure AD Security Group (Max 3) please provide the Azure Object ID of each Azure AD Security Group.

Azure AD Group Object ID	Group Type
	Recorded Users
	Supervisors
	Admins

To retrieve the Azure Object ID of each Azure AD Group, you can use the "Get-AzADGroup" CMDLet, for example:

```
Get-AzADgroup -DisplayName "StratusVerbaRecorded"
```

This returns the below and here we can retrieve the object Id for this group

```
SecurityEnabled : True
MailNickname   : 00000000-0000-0000-0000-000000000000
ObjectType      : Group
Description     : StratusVerbaRecorded
DisplayName     : StratusVerbaRecorded
Id              : 7c50e42c-140f-4860-b0eb-f739e3288a9f
Type            :
```

For example:

Azure AD Group Object ID	Group Description
7c50e42c-140f-4860-b0eb-f739e3288a9f	Recorded Users
	Supervisors
	Admins

9 ROLE BASED ACCESS CONTROL

This section details the default Role Based Access Control deployed as standard for each of the three User Groups (Recorded, Supervisor and Admin).

If you require a bespoke setup of RBAC Roles and Permissions please discuss this with your sale representative within Luware and further information can be shared upon request.

9.1 RECORDED USER PERMISSIONS

RBAC Permissions
Can Playback own Conversations
Can export own Conversations
Modify own Search Portal

9.2 SUPERVISOR PERMISSIONS

Please note it is assumed Supervisors are not recorded persons however supervisors can be enabled for recording if required.

RBAC Permissions
Can Playback All Conversations
Can export All Conversations
Modify own Search Portal
Sharing of conversations
Annotation of conversations
Enable/Disable Legal hold of Conversations

9.3 ADMIN PERMISSIONS

Please note it is assumed Admins are not recorded persons however supervisors can be enabled for recording if required

RBAC Permissions
NO CONVERSATION ACCESS
User Read: Update and Delete
Group Read: Update and Delete
Extensions: Read, Update and Delete
Roles: Read Only
AD Synch Profiles: Read Only
Identity Providers: Read Only
Storage Targets: Read and Update only
Retention Policies: Read and Update only

10 CONVERSATION RETENTION SETTINGS

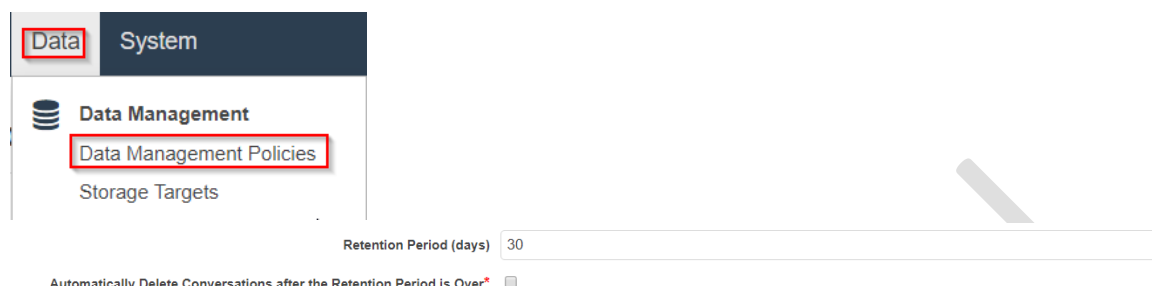
Luware Stratus Recording will upload all recorded conversations to the customers Azure Storage Account File Share Storage.

A retention period can be configured by Luware Stratus Recording to delete conversations after a certain period of time.

Please enter the number of days you would like to keep recorded conversations:

Days to Keep Conversations

By default, Luware Stratus Recording will not implement retention delete settings, however the customers "Admin" users can edit the retention policy settings if required.



Luware Stratus Recording also allows for customers to create more granular archiving policies leveraging the customers' lower tier storage platform in Azure, further information can be provided upon request.

11 MICROSOFT TEAMS COMPLIANCE POLICIES

This section details the customer preconditions that must be followed in order to integrate the customers Microsoft Teams Tenant users for Compliance Recording with Luware Stratus Recording hosted service.

This section assumes the following has been read and understood from the previous sections:

- Azure Storage Requirements and optionally Data at Rest Signing and Encryption options
- Azure AD User Synchronization Requirements
- Luware Stratus Recording RBAC Requirements

11.1 CREATE MICROSOFT TEAMS COMPLIANCE POLICIES

This section details the Microsoft Teams Compliance policies that the customer needs to create to enable Teams Compliance Recording for users.

Before detailing the PowerShell commands that are needed to be run within the customers Azure AD Tenant, there are two concepts that need to be understood.

- **Fail Close** = When a Recorded Microsoft Teams user is under strict compliance (i.e. mandated to be recorded at all times) then if the recording fails for any reason the call will not be allowed.
- **Fail Open** = Opposite of Fail Close – i.e. if recording fails for any reason the call will still be allowed to take place.

Microsoft Teams Compliance Recording Policies allows for the creation of Fail Open and Fail Close Policies, Luware has provided a script that can be used to create the needed policies and output post tasks that need to be performed.

All native teams call recording is performed via Azure Bot Channel currently hosted in North Switzerland, customers leverage cross tenant access to the Luware Stratus Recording Azure Teams Bot which has the global ID of: "39f71ecc-0552-4517-a36f-4b5a533e03d3"

In all cases below please ensure you have installed Skype Bus Connector PowerShell module (<https://www.microsoft.com/en-us/download/details.aspx?id=39366>)

11.2 SCRIPTED CREATION OF COMPLIANCE POLICIES

Luware has provided a script that can simplify the Microsoft Teams Compliance Policies. How to use the script is detailed below (the script can be found towards the bottom of this document) – If the customer does not wish to use the script and to perform the steps manually please skip this section and go to 11.3.

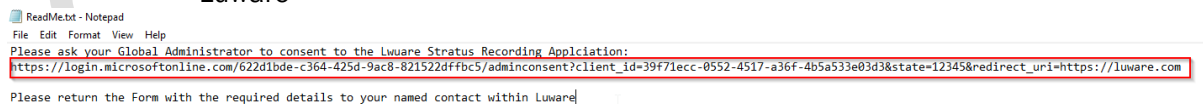
1. Modify the Variables of the script to your preference:
 - a. using 1 for `$FailClose` will create a Fail Close Policy, using 0 will create a fail open policy, you can create as many policies as you desire (recommendation is to use fail open to begin with)
 - b. The UPN should be a native O365 Domain (you can use the onmicrosoft.com domain for this – on-premises directory synced hybrid Application Instances will be tested soon)
 - c. Rest of the variables are self-explanatory

```
$FailClose = 0
$AppUPN = "<Your Preferred UPN Here>"
$PolicyName = "<Your Policy Name Here>"
$PolicyDescription = "<Your Policy Description Here>"
$AppInstanceDisplayName = "<Your App Instance Display Name Here>"
```

EXAMPLE of Fail Open:

```
$PolicyName = "Fail Open Recording"
$PolicyDescription = " Fail Open Recording"
$AppInstanceDisplayName = " Fail Open Recording"
$AppUPN = "FailOpenRecording@luware.onmicrosoft.com"
$FailClose = 0
```

2. Once satisfied with the Variable values, please execute the script under an account that is allowed to create Application Instances, Teams Compliance Policies and Applications
3. The script will take 20 to 30 secs to execute and will produce a text file with post actions that MUST be performed by the Customers Azure Global Administrator
 - a. Prompted to consent to the Luware Stratus Recording Bot application URL
 - b. Promoted to return this form back to your named technical point of contact within Luware



The permissions consent will prompt for the permissions shown below:



Permissions requested Accept for your organization

Luware Stratus Teams Recording
emea.luware.cloud

This application is not published by Microsoft or your organization.

This app would like to:

- ✓ Sign in and read user profile
- ✓ Access media streams in a call as an app
- ✓ Initiate outgoing 1 to 1 calls from the app
- ✓ Initiate outgoing group calls from the app
- ✓ Join group calls and meetings as an app
- ✓ Join group calls and meetings as a guest
- ✓ Read directory data
- ✓ Read all groups
- ✓ Read online meeting details
- ✓ Read and create online meetings
- ✓ Read all users' full profiles
- ✓ Read and write all users' full profiles

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Cancel

Accept

11.3 MANUAL CREATION OF COMPLIANCE POLICIES

If the customer prefers to run through the Teams Compliance Policy Creation process manually, details are provided below.

11.4 WHITE LISTING LUWARE STRATUS RECORDING APPLICATION

The first thing we need to perform is creating a White Listed Application Instance
 Open PowerShell as Administrator:

1. Use the following commands

- a. `Import-Module SkypeOnlineConnector`
- b. `$userCredential = get-Credential`
 Login form prompted - sign in with the teams tenant administrator account
- c. `$teamsSession = New-CsOnlineSession -Credential $userCredential -Verbose`
- d. `Import-PSSession $teamsSession`
- e. `New-CsOnlineApplicationInstance -UserPrincipalname <UPN> -DisplayName <displayName> -ApplicationId "39f71ecc-0552-4517-a36f-4b5a533e03d3"`

This command adds the bot as an application.

The UPN should be a unique name for the bot

e.g. recordingbot@customer.onmicrosoft.com

!! The command return the successful registration. The result contains the **Object ID - save it for the next command**

- f. `Sync-CsOnlineApplicationInstance -ObjectId <ObjectId>`

The application is now whitelisted in your tenant. We can now proceed to create the needed Microsoft Teams Compliance Policies.

11.4.1 CREATING MICROSOFT TEAMS COMPLIANCE POLICY

We continue from the previous section, in this section we create the Teams Compliance Policy that is desired. – **You will need the object ID value from the previous section!**

1. Create and set recording application for the policy (**default fail close**)

- a. `New-CsTeamsComplianceRecordingPolicy -Tenant '<TenantId>' -Enabled $true -Description '<Policy Description>' -Identity '<PolicyName>'`
- b. `Set-CsTeamsComplianceRecordingPolicy -Tenant '<TenantId>' -Identity '<PolicyName>' -ComplianceRecordingApplications @(New-CsTeamsComplianceRecordingApplication -Tenant '<TenantId>' -Parent '<PolicyName>' -Id '<ObjectId>')`

1. In order to create a **fail open policy**, follow the steps below:

Name	Description	Default Setting
RequiredBeforeCallEstablishment	Defines if the bot has to join the call before the recorded user can place or receive calls	1 (On)
RequiredBeforeMeetingJoin	Defines if the bot has to join the call before the recorded user can join the meetings	1 (On)
RequiredDuringCall	Defines if the recorded user will be disconnected from the call if the recorder bot connection is lost	1 (On)
RequiredDuringMeeting	Defines if the recorded user will be disconnected from the meetings if the recorder bot connection is lost	1 (On)

- a. `New-CsTeamsComplianceRecordingPolicy -Tenant '<TenantId>' -Enabled $true -Description '<Policy Description>' -Identity '<PolicyName>'`
- b. `Set-CsTeamsComplianceRecordingPolicy -Tenant '<TenantId>' -Identity '<PolicyName>' -ComplianceRecordingApplications @(New-CsTeamsComplianceRecordingApplication -Tenant '<TenantId>' -Parent '<PolicyName>' -Id '<ObjectId>' -RequiredBeforeCallEstablishment $false -RequiredDuringCall $false -RequiredBeforeMeetingJoin $false -RequiredDuringMeeting $false)`

Please note you can change the policy fail open / fail close settings by using the command:

```
Set-CsTeamsComplianceRecordingApplication -
Identity '<PolicyName>/<ComplianceApplicationId>' -
RequiredBeforeMeetingJoin 0 -
RequiredBeforeCallEstablishment 0 -RequiredDuringMeeting 0 -
RequiredDuringCall 0
```


11.4.2 CONSENT PERMISSIONS TO LUWARE STRATUS RECORDING BOT

This section provides the URL that needs to be provided to the Azure Global Administrator in order for the Luware Stratus Recording Bot to be able to perform the needed functions.

Please replace <CUSTOMER TENANT ID> with the actual Azure Tenant ID of the customer.

https://login.microsoftonline.com/<CUSTOMER TENANT ID>/adminconsent?client_id=39f71ecc-0552-4517-a36f-4b5a533e03d3&state=12345&redirect_uri=https://luware.com

11.5 GRANTING COMPLIANCE POLICIES TO USERS

Once the desired policies have been created successfully (either via script or manually), the final step is to grant the desired Teams compliance Recording Policies to the compliance mandated Teams Users.

1. Grant the policy to a user (takes several minutes to be applied)
 - a. `Grant-CsTeamsComplianceRecordingPolicy -Identity '<User's UPN>' -PolicyName '<PolicyName>'`
2. The granted policy can be verified by the following command
 - a. `Get-CsOnlineUser -Identity '<User's UPN>' | Select-Object -ExpandProperty 'TeamsComplianceRecordingPolicy'`

12 ACCESSING LUWARE STRATUS RECORDING PORTAL

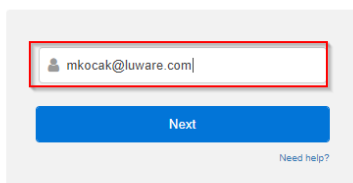
Once all the previous sections have been discussed, agreed, implemented, and this document with the required details has been returned to your technical point of contact, each of the three user types can access the Luware Stratus Recording Portal by browsing to:

<https://chteamsrec01.emea.luware.cloud>

The synchronized users (detailed in section 3.1) login name is their User Principal Name, once the user name is entered and “Next” is selected, the user will be redirected back to the customers ADFS Services (or O365 Authentication Services if there is no customer on-premises ADFS)

From here the traditional SAML / ADAL based authentication process takes place:

- User enters User Principal Name to the user login field within the portal:



The software is licensed to: Luware AG
 Version: 9.5.0.5899
 © 2020 Verint Systems Inc. © 2020 Verba Technologies Ltd. All Rights Reserved Worldwide.

- Users select next and is redirected to the customers Azure AD Authentication Services, which can then in turn re-direct to the customers on-premises ADFS Services if the user is enabled for on-premises ADFS (and is likely Directory Synced).



Sign in with your organizational account

Sign in

- The user will enter the Azure AD or On-premises Active Directory User Password and is then authenticated and re-directed back to the Luware Stratus Portal and sign in is successful.

Please discuss, if required, portal training with your sales representative within Luware.

12.1 RETURN THIS DOCUMENT

Before returning this document to your named point of technical contact within Luware, please ensure the requirements and conditions are met (as detailed in previous sections) and all required details are gathered and supplied in this document where requested.

Please return this document using a secure method to your named point of technical contact within Luware.

13 APPENDIX

Luware PowerShell Script to create Customer Teams Compliance Policies:

```
$UserCredential = Get-Credential
$SfbSession = New-CsOnlineSession -Credential $UserCredential -Verbose
Import-PSSession -Session $SfbSession -AllowClobber

$PolicyName = "<Your Policy Name Here>"
$PolicyDescription = "<Your Policy Description Here>"
$AppInstanceDisplayName = "<Your App Instance Display Name Here>"
$AppUPN = "<Your Preferred UPN Here>"
$FailClose = 1

<# EXAMPLE of Fail Open:

$PolicyName = "Test Fail Open"
$PolicyDescription = "Test Fail Open"
$AppInstanceDisplayName = "Test Fail Open"
$AppUPN = "TestFailOpen@luware.onmicrosoft.com"
$FailClose = 0
#>

<# EXAMPLE of Fail Close:

$PolicyName = "Test Fail Close"
$PolicyDescription = "Test Fail Close"
$AppInstanceDisplayName = "Test Fail Close"
$AppUPN = "TestFailClose@luware.onmicrosoft.com"
$FailClose = 1
#>

$StratusBotAppID = "39f71ecc-0552-4517-a36f-4b5a533e03d3"
[STRING]$CustomerTenantID = (Get-CsTenant).TenantID.Guid

$newapp = New-CsOnlineApplicationInstance -UserPrincipalname $AppUPN -DisplayName
$AppInstanceDisplayName -ApplicationId $StratusBotAppID
sleep 10
Sync-CsOnlineApplicationInstance -ObjectId $newapp.ObjectId
sleep 10
New-CsTeamsComplianceRecordingPolicy -Tenant $CustomerTenantID -Enabled $true -Description
$PolicyDescription -Identity $PolicyName

if($FailClose -eq 1)
{
    $ComplianceApp = New-CsTeamsComplianceRecordingApplication -Tenant $CustomerTenantID -
Parent $PolicyName -Id $newapp.ObjectId
}
else
{
    $ComplianceApp = New-CsTeamsComplianceRecordingApplication -Tenant $CustomerTenantID -
Parent $PolicyName -Id $newapp.ObjectId -RequiredBeforeCallEstablishment $false -
RequiredDuringCall $false -RequiredBeforeMeetingJoin $false -RequiredDuringMeeting $false
}

Set-CsTeamsComplianceRecordingPolicy -Tenant $CustomerTenantID -Identity $PolicyName -
ComplianceRecordingApplications @($ComplianceApp) -Enabled $true

$ConsentUrl =
"https://login.microsoftonline.com/$CustomerTenantID/adminconsent?client_id=$StratusBotAppID&
state=12345&redirect_uri=https://luware.com"

Clear-Content .\ReadMe.txt
"Please ask your Global Administrator to consent to the Luware Stratus Recording
Application:" >> .\ReadMe.txt
"$ConsentUrl" >> .\ReadMe.txt
"" >> .\ReadMe.txt
"Please return the Form with the required details to your named contact within Luware" >>
.\ReadMe.txt
notepad.exe .\ReadMe.txt

PAUSE
```