

White Paper

External Identity Provider

Table of Content

Introduction	3
Purpose and target audience	4
External IDP overview.....	5
Login and authentication overview.....	5
External IDP integration.....	7
Prerequisites	7
External IDP configuration example	7
Adding an external IDP in XProtect VMS.....	17
VMS roles and external IDP users.....	20
Claim-based XProtect VMS role linking.....	20
External IDP users in the XProtect VMS.....	22
Effective roles.....	23
Client experience.....	25
XProtect Smart Client and Management Client	25
External IDP authentication	25
No Claims, or claims not added to roles.....	29
XProtect Web Client and Mobile client	30
XProtect Mobile Client	34
User management and audit logs.....	37
Deleting and disabling external IDP users	37
Audit logs	38
External IDP user limitations	39
Milestone Federated Architecture.....	39
Milestone Interconnect	39
Benefits and summary	40

Introduction

Milestone's XProtect VMS products are designed for large-scale, high-security installations and are often deployed in places where user management with Microsoft on-prem Active Directory or the XProtect VMS' built-in basic users don't meet the customer requirements for user management and authentication.

To address these customer requirements, the XProtect VMS products support an external Identity Provider (IDP) via the [OpenID Connect \(OIDC\)](#) and the [OAuth2](#) protocols and standards.

When integrating an external IDP with the XProtect VMS, most of the user management, including user provisioning and roles assignment, can be managed directly from the external IDP. This allows customers to have a central place to manage their users throughout their organization, regardless of what applications the users interact with or their choice of platform or operating system, for example, Microsoft Windows, Linux, Apple's macOS, Smart Phones or a browser-based interface.

Purpose and target audience

The purpose of this white paper is to provide insights to the configuration, usage and benefits of integrating an external IDP with Milestone XProtect VMS.

This white paper should enable the reader to understand:

- What must be pre-configured in the external IDP to allow the XProtect VMS integration
- How the external IDP and the XProtect VMS are integrated
- What must be configured to automatically link the external IDP users to XProtect VMS roles
- How external IDP users can be added manually to XProtect VMS roles in cases where they cannot be automatically linked to the VMS roles

The primary audience for this white paper is organizations that wish to deploy a Milestone XProtect VMS and have it integrated with an OIDC/OAuth2 compliant Identity Provider chosen by the organization.

The target group might include (but is not limited to) the following audiences:

- Surveillance system and IT architects and designers
- Surveillance system and IT project consultants
- Surveillance system and IT administrators

This white paper should enable the reader to understand the principles behind integrating an external IDP with the XProtect VMS, how external IDP users can be linked automatically to the XProtect VMS roles based on user's claims from the external IDP, and how the user experience will be when accessing the XProtect VMS as an external IDP user.

The white paper assumes that the reader has a general understanding of the XProtect VMS and the roles functionality. Furthermore, it is assumed that the reader has a detailed understanding of how the selected Identity Provider is configured to provide the XProtect VMS with the information needed for the XProtect VMS integration.

External IDP overview

A key functionality in the XProtect VMS is secure user authentication for any user who wants to access the XProtect VMS using one of the XProtect clients, the MIP SDK, or the supported APIs.

In the past, users have traditionally been managed in an organization's on-premises Microsoft Active Directory (AD), or alternatively for installations that do not have an AD, as local Windows users or as basic users in the XProtect VMS.

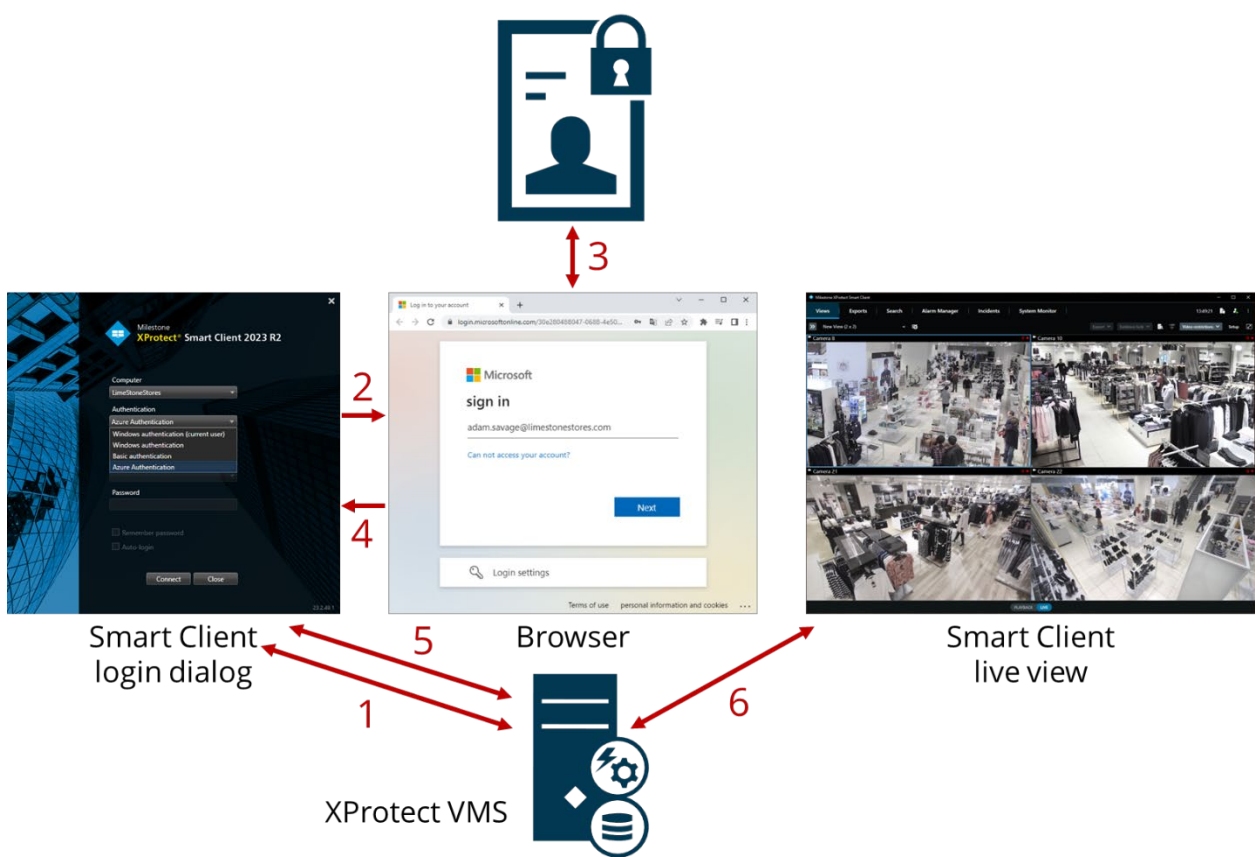
However, nowadays many organizations have users that use a plethora of different products, services and solutions from many different vendors, running in browsers etc. on multiple platforms like PCs, MACs, or Smart Phones. These organizations need a centralized user-management system that works with the different equipment, platforms and interfaces used – which is not the case with the on-premises AD. Therefore, they chose to use another Identity Provider to manage their users and their permissions.

When these customers acquire an XProtect VMS, they will of course want to use the same Identity Provider as the one that they already have chosen and installed with their XProtect VMS. This is achieved by creating an integration between the Identity Provider and the XProtect VMS.

Login and authentication overview

When the Identity Provider and the XProtect VMS integration have been configured, the high-level login and authentication flow will look like this.

1. When the XProtect VMS address has been entered in the VMS client's login dialog, the authentication options are retrieved from the XProtect VMS and listed in the login dialog
2. Choosing the external IDP option and clicking 'Connect', opens a browser window that displays the external IDP's login page
3. Entering the username and password authenticates the user with the external IDP
4. After successful authentication, an OAuth token is transferred from the browser to the VMS client
5. Using the external IDP's OAuth token, the VMS client authenticates the user in the VMS, which then returns a VMS security token and the configuration for the user
6. The VMS client is now started and provides access to the VMS resources that the user has permissions for



External IDP integration

The integration of an external IDP into the XProtect VMS requires the external IDP to support Open ID Connect (OIDC) and OAuth2. Furthermore, depending on the specific Identity Provider used, a varying amount of configuration of both the Identity Provider and XProtect VMS is required to allow the XProtect VMS to trust and communicate with the external IDP, and likewise for the external IDP to allow log-in requests coming from the XProtect VMS and the XProtect clients.

The following information and settings must be configured in both the external IDP and the XProtect VMS:

- Client ID
- Client Secret
- Address of external IDP
- User Claims (optionally)
- Redirect URI's

When properly configured, the external IDP will be available to users as an additional authentication option in the XProtect clients. Users who choose to authenticate using the external IDP will be redirected to log in on the chosen IDP's login page in a browser.

Prerequisites

The following prerequisites must be met to integrate the external IDP into the XProtect VMS:

- The client ID and secret for use with the XProtect VMS must be created in the external IDP
- The authentication address for the external IDP must be known
- The redirect URIs to the XProtect VMS must be configured in the external IDP
- Optionally, VMS related claims must be configured for the users or groups in the external IDP
- The XProtect VMS must run version 2023 R1 or later
- The XProtect VMS must be fully configured with certificates to ensure all communication is done over encrypted https.
 - If this is not done, most external IDPs will not accept requests from the XProtect VMS and its clients, or part of the communication flow and security token exchange will fail
- The XProtect VMS and all client computers or smart phones that should use the external IDP must be able to contact the external IDP's login address

External IDP configuration example

Disclaimer: Since the Identity Provider product or service is provided by a 3rd party company and not by Milestone Systems, and because there are many different Identity Provider products and services available, Milestone cannot document how the different Identity Providers are configured or offer support on how to configure the chosen Identity Provider for usage with the XProtect VMS.

However, for the content of this white paper, Milestone's Microsoft Entra ID account (Previously named Azure Active Directory) has been configured to enable an XProtect VMS IDP

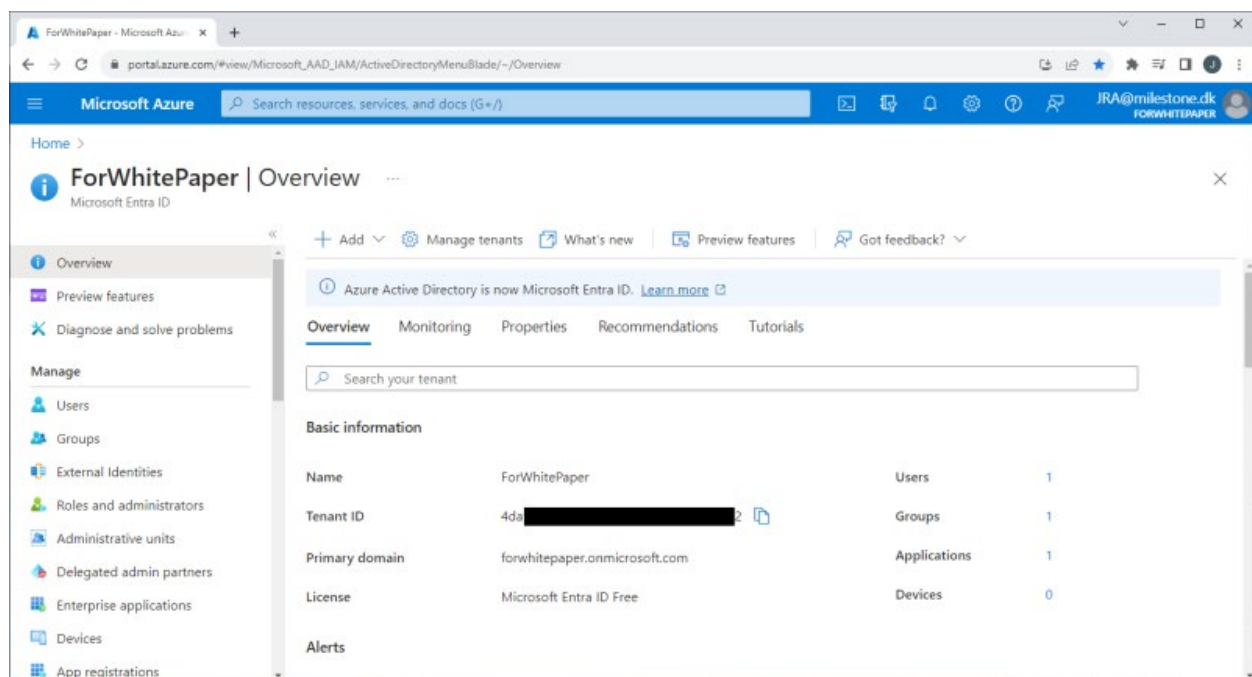
integration, and the text and screenshots that apply to the Microsoft Entra ID configuration provide an example of what needs to be configured in Microsoft Entra ID to allow the XProtect VMS to integrate user authentication with Microsoft Entra ID.

The screenshots and descriptions in this white paper will only provide a very high-level overview of the steps and areas that must be configured for the XProtect VMS to use Microsoft Entra ID's IDP functionality. Furthermore, please note that Microsoft Entra ID's interface, configuration flow and settings might have changed after the publication of this white paper.

The following steps must be completed in Microsoft Entra ID to allow the XProtect VMS IDP integration:

1. An Entra ID tenant must be created, and for the Entra ID tenant the following steps must be completed
2. An Enterprise application must be created
3. An App registration must be created
4. A secret must be created for the registered app
5. Redirect URIs for the XProtect VMS servers must be set for the app
6. A role must be created for the registered app
7. One or more users must be added to the enterprise application, and they must have a role assigned

Tenant Created



With the tenant created ("ForWhitePaper") the tenant is selected, and an overview can be seen.

Add Enterprise application

An Enterprise application is added by selecting 'Enterprise applications' and clicking '+ Create your own application'. In the new dialog, give the application a name, and select the radio button option called 'Integrate any other application you don't find in the gallery (Non-gallery)'.

The screenshot displays two overlapping windows from the Microsoft Azure portal. The top window, titled 'Enterprise applications - Microsoft Azure', shows the 'All applications' page. The left sidebar contains navigation links for Overview, Diagnose and solve problems, Manage (All applications, Application proxy, User settings, App launchers, Custom authentication extensions), and Security (Conditional Access, Consent and permissions). The main content area shows a search bar, filters for 'Enterprise Applications', and a table with 0 applications found. The bottom window, titled 'Create your own application - Microsoft Azure', shows the 'Create your own application' dialog. It includes a 'Got feedback?' link, a description of the Microsoft Entra ID App Gallery, a search bar, and a list of cloud platforms (Amazon Web Services (AWS) and Google Cloud Platform). The dialog also asks for the application name (VMS-forwhitepaper) and the purpose (Integrate any other application you don't find in the gallery (Non-gallery)).

Enterprise applications | All applications

ForWhitePaper - Microsoft Entra ID

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications
- Application proxy
- User settings
- App launchers
- Custom authentication extensions (Preview)

Security

- Conditional Access
- Consent and permissions

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

Search by application name or ob... Application type == Enterprise Applications Application ID starts with Add filters

0 applications found

Name	Object ...	Application ID	Homepage U...	Created on	Cert...	Ac...	Identifier URI (E...
No results							

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

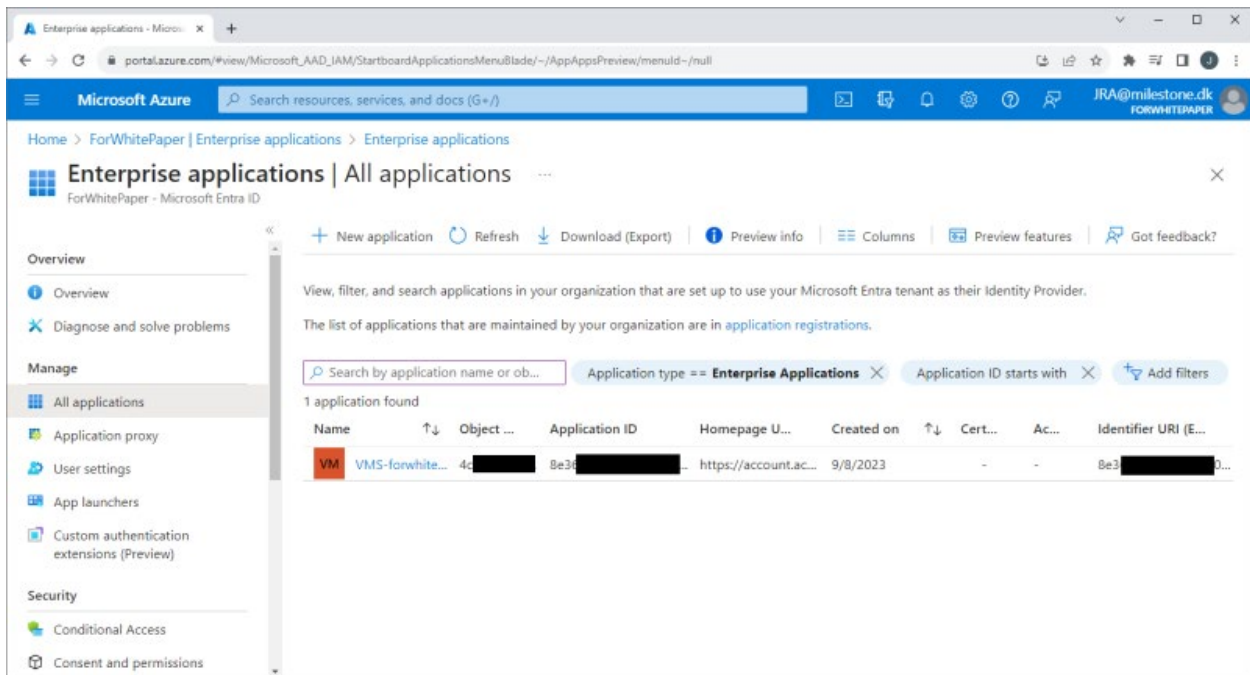
What's the name of your app?

VMS-forwhitepaper

What are you looking to do with your application?

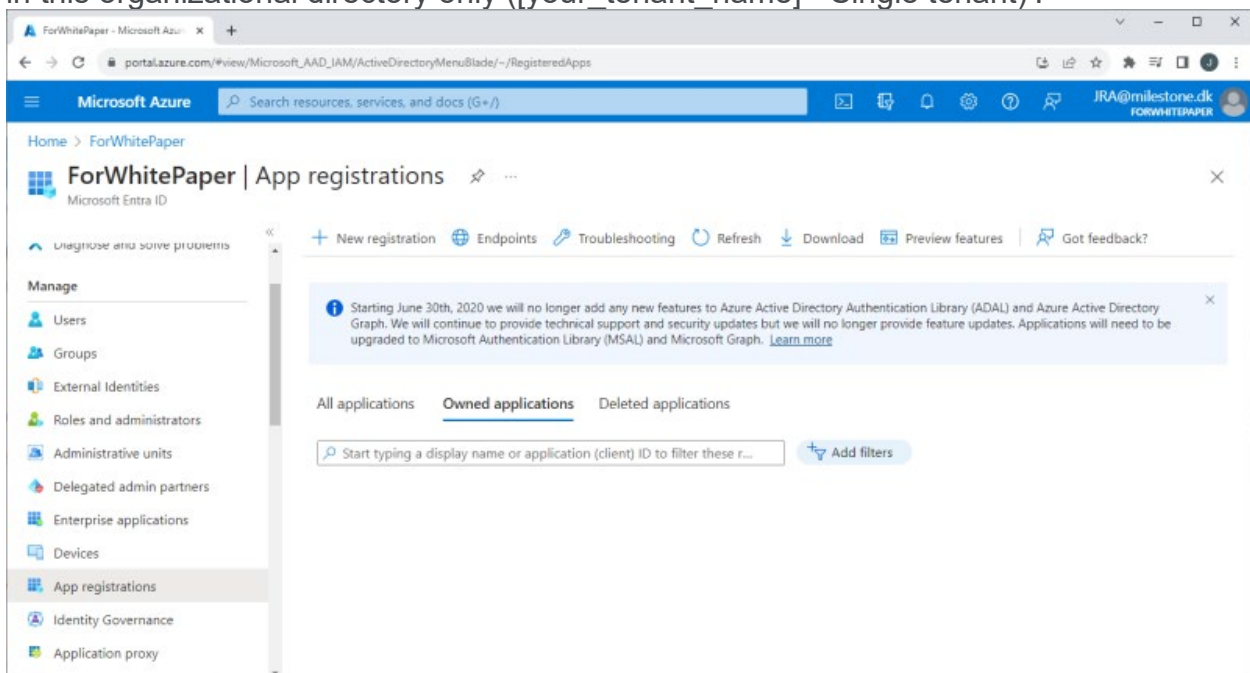
- ☐ Configure Application Proxy for secure remote access to an on-premises application
- ☐ Register an application to integrate with Microsoft Entra ID (App you're developing)
- ☒ Integrate any other application you don't find in the gallery (Non-gallery)

Create



Add App registration

An app is registered by selecting 'App registration' and clicking '+ New registration'. In the new page, give the application a name and select the radio button option called 'Accounts in this organizational directory only ([your tenant name] - Single tenant)'.

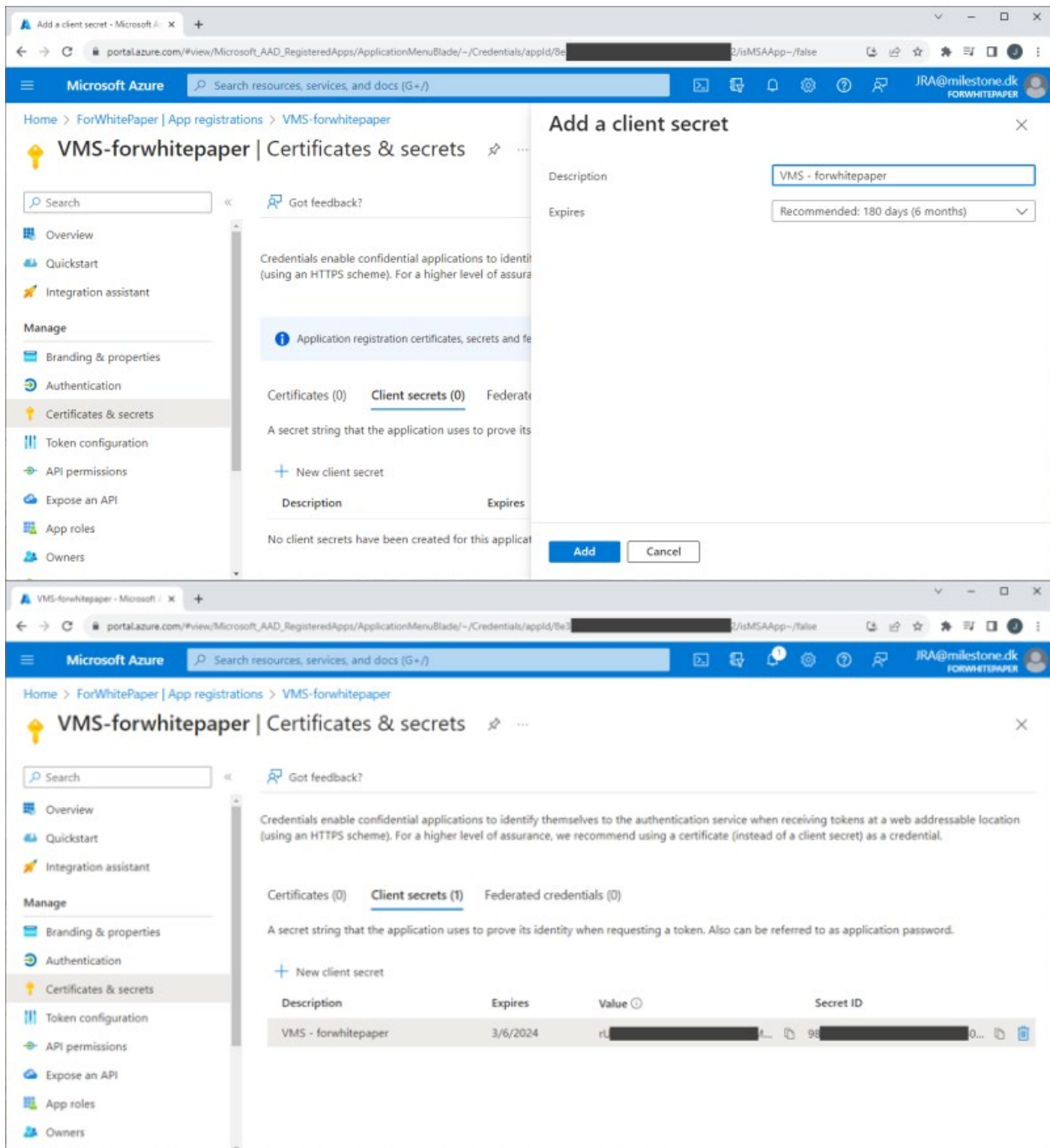


The top screenshot shows the 'Register an application' page in the Microsoft Azure portal. The 'Name' field is filled with 'VMS-forwhitepaper'. Under 'Supported account types', the option 'Accounts in this organizational directory only (ForWhitePaper only - Single tenant)' is selected. A 'Register' button is at the bottom.

The bottom screenshot shows the 'App registrations' page. A notification banner at the top states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)'. Below the notification, the 'Owned applications' tab is active, showing one application found: 'VMS-forwhitepaper' with application ID '8e366...' and creation date '9/8/2023'. The 'Certificates & secrets' column shows a green checkmark and the word 'Current'.

Set app secret

A secret for the app is set by selecting 'Certificates & secrets' and clicking '+ New client secret'. In the new dialog, enter a description and specify when the secret expires.



Important: The secret value is only shown on this page immediately after it is created and it cannot be viewed again after navigating away from the page. This secret is needed in the XProtect VMS for the external IDP integration, so make sure to copy it and save it somewhere safe. If the secret is lost or you forgot to copy it, it is possible to create a new one and use it going forward.

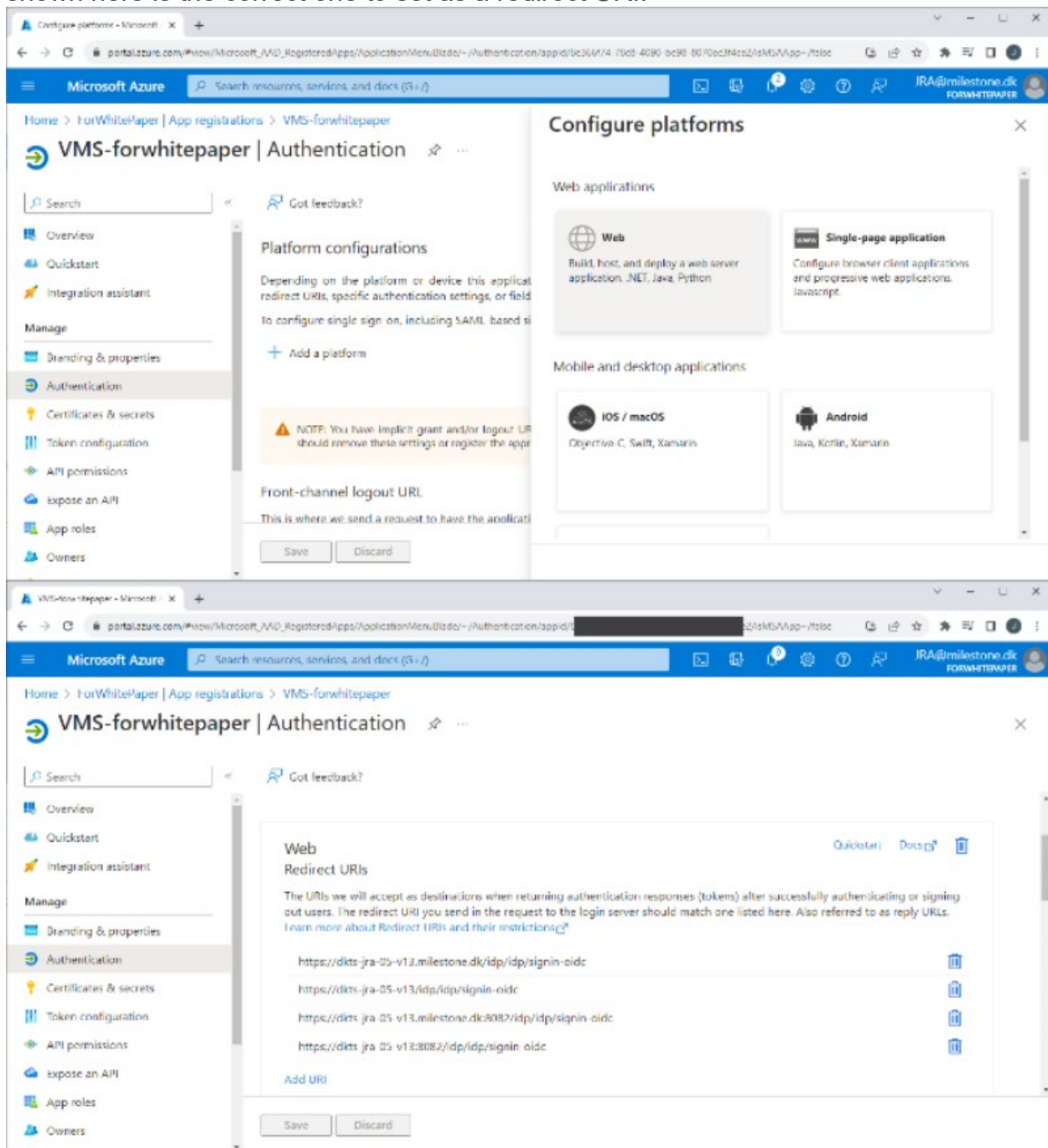
Set redirect URIs

Redirect URIs are set for the app by selecting 'Authentication' and clicking '+ Add a platform'. In the new dialog shown, select 'Web' and enter the addresses and ports to the XProtect management server and mobile server. Depending on how the XProtect VMS is accessed, how the network, servers and Microsoft Active Directory is configured, several redirect URIs may be needed.

The redirect URI usually follows this format:

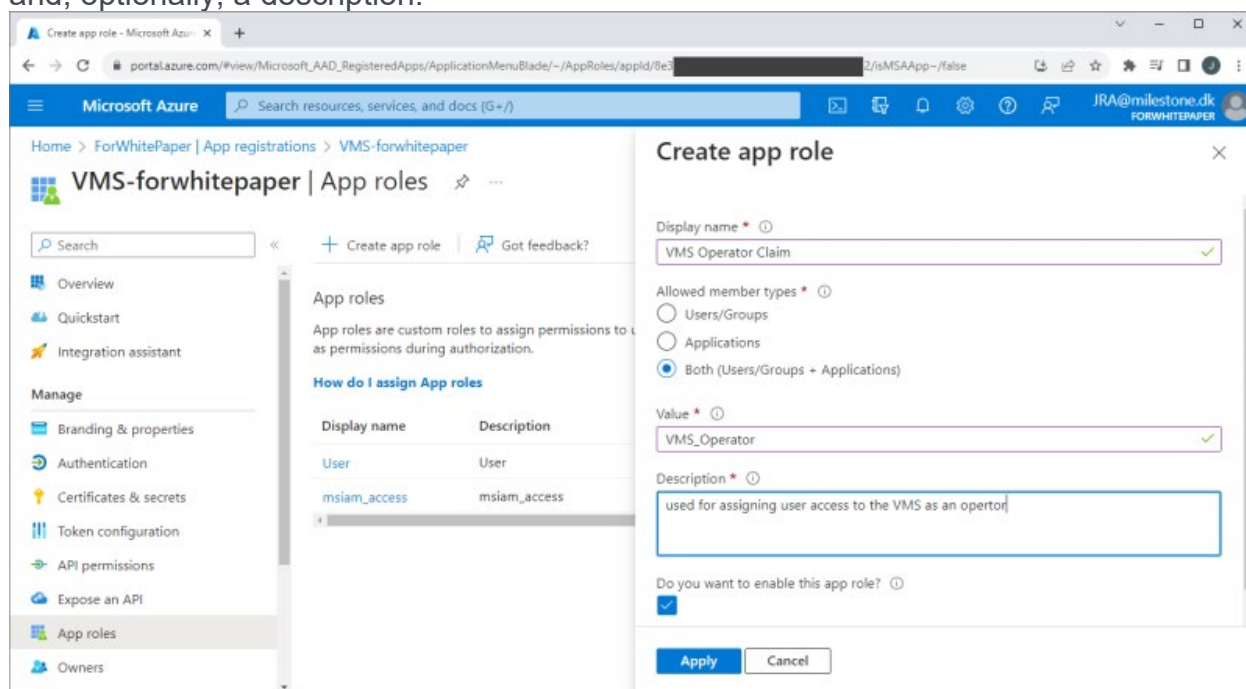
- Mobile server:
 - “https://[server_name]:[mobile_port]/idp/idp/signin-oidc”
 - “https://[server_name].[domain_name]:[mobile_port]/idp/idp/signin-oidc”
- Management server:
 - “https://[server_name]/idp/idp/signin-oidc”
 - “https://[server_name].[domain_name]/idp/idp/signin-oidc”

If the redirect URI is configured incorrectly, an error message will be shown during authentication, stating that the redirect URI is incorrect. For example: ‘The redirect URI https://vmsserver.limestonestores.com:8082/index.html/idp/idp/signin-oidc specified in the request does not match the redirect URIs configured for the application...’. The address shown here is the correct one to set as a redirect URI.



Create role

Roles are created for the app by selecting 'App roles' and clicking '+ Create app role'. In the new dialog shown, give the role a name, select allowed member types, enter a value, and, optionally, a description.



The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane is open, showing the 'App roles' section under 'VMS-forwhitepaper'. The main area displays the 'Create app role' dialog. The dialog has the following fields and options:

- Display name ***: VMS Operator Claim (with a green checkmark)
- Allowed member types ***: Both (Users/Groups + Applications) (selected with a radio button)
- Value ***: VMS_Operator (with a green checkmark)
- Description ***: used for assigning user access to the VMS as an operator
- Do you want to enable this app role?**: Yes (checked with a checkbox)

At the bottom of the dialog are 'Apply' and 'Cancel' buttons. In the background, a table lists existing app roles:

Display name	Description
User	User
msiam_access	msiam_access

The roles and their values created here, can be used as claims in the XProtect VMS to automatically link the Microsoft Entra ID users to the XProtect VMS roles. This, though, requires that the Microsoft Entra ID user that is added to the app in the next step, is assigned this app role.

Adding users or groups to the enterprise application

Note: It is assumed that the users or groups have already been added or created in the Entra ID tenant.

Tenant users or groups are added to the enterprise application by first navigating to the created VMS enterprise application in Entra ID. Then select 'Users and groups' and clicking '+ Add user/group'. In the new dialog shown, select the user or group and then select a role for the user or the group.

VMS-forwhitepaper - Microsoft

portal.azure.com/#view/Microsoft_AAD_IAM/ManagedAppMenuBlade/~Users/objectId/4...

Microsoft Azure

Search resources, services, and docs (G+)

JRA@milestone.dk

Home > VMS-forwhitepaper

VMS-forwhitepaper | Users and groups

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

+ Add user/group

Edit assignment

Remove

Update credentials

Columns

Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#).

First 200 shown, to search all users & gro...

Display Name	Object Type	Role assigned
No application assignments found		

Add Assignment - Microsoft Az...

portal.azure.com/#view/Microsoft_AAD_IAM/AddAssignmentBlade/objectId/4cb537f0-0ff1-40b6-b638-1ecc36c188ed

Microsoft Azure

Search resources, services, and docs (G+)

JRA@milestone.dk

Home > VMS-forwhitepaper | Users and groups >

Add Assignment

ForWhitePaper

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

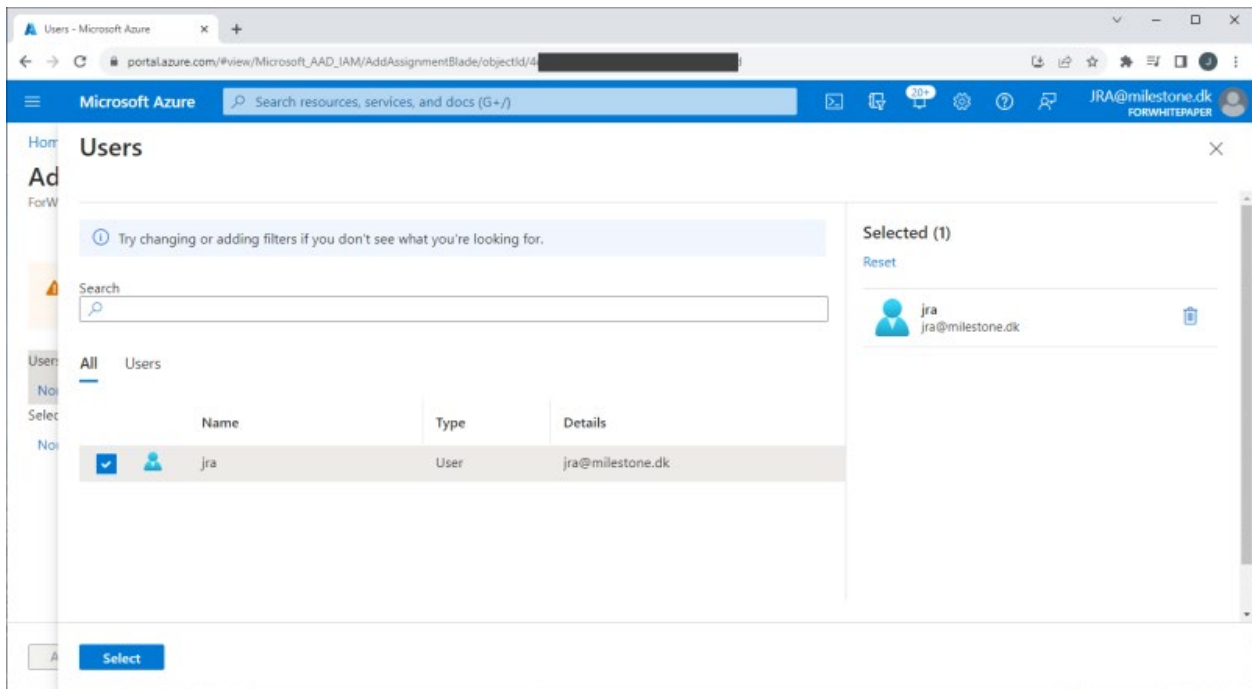
Users

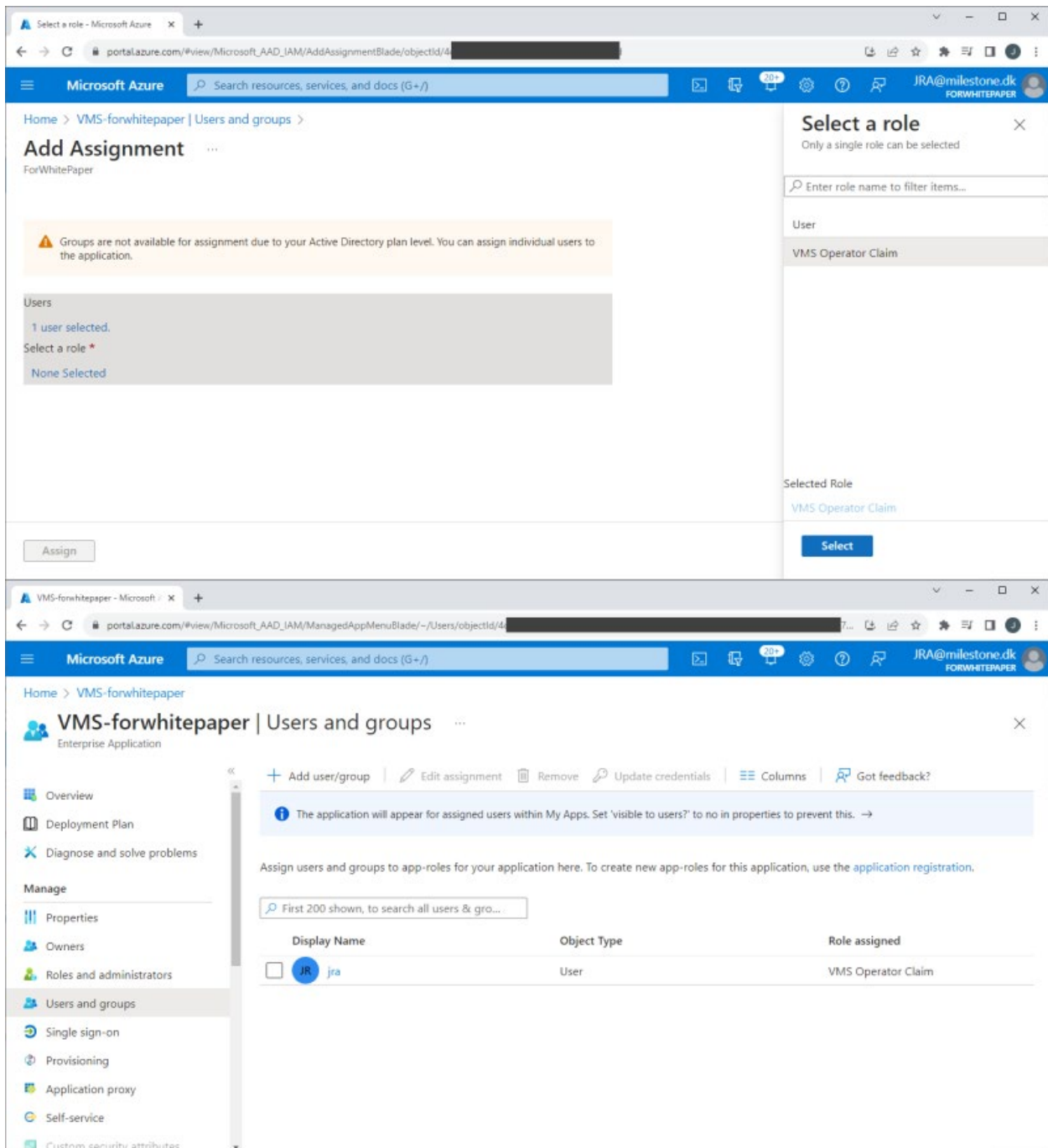
None Selected

Select a role *

None Selected

Assign





Adding an external IDP in XProtect VMS

Adding an external IDP to the XProtect VMS is fairly straightforward and only requires configuration of a few parameters for the external IDP:

- Client ID – provided by the external IDP
- Client Secret – configured in, and provided by, the external IDP
- Authentication authority – address of the external IDP
- Optionally
 - A claim provided by the external IDP that can be used for the XProtect VMS user name

- For example, the claim “email” for a user is myuser@mydomain.com. When this user logs in to the XProtect VMS using the external IDP, a basic user will be created in the XProtect VMS and listed as myuser@mydomain.com

The external IDP integration is configured on the ‘External IDP’ tab in the XProtect Management Client’s ‘Options’ dialog.

Options

User Settings External IDP Evidence Lock Audio Messages Privacy settings Access Control Settings Analytics < >

External IDP

Enabled	Name	Authentication authority
<input checked="" type="checkbox"/>	Azure Authentication	https://login.microsoftonline.com/30e28...

Add Edit Remove

Registered claims

External IDP	Claim name	Display name	Case sensitive
--------------	------------	--------------	----------------

Add Edit Remove

Redirect URIs for web clients

URI

Add Edit Remove

Help OK Cancel

Edit external IDP

✕

☒ Enabled

Name:

Azure Authentication

Client ID:

9b347d67222-8b9a-454f-b696-3faf771a009b

Client secret:

.....

☒ Set client secret

Callback path:

/signin-oidc

Authentication authority:

https://login.microsoftonline.com/6777ef47-0688-4e50-97ec-d0bfe70c3793/v2.0/

☒ Prompt user for login

Claim to use to create user names:

email

Scopes:

Add

Edit

Remove

OK

Cancel

VMS roles and external IDP users

Users from the external IDP cannot be added to the XProtect VMS roles in the same way as Microsoft Active Directory (AD) users, local Windows users, or XProtect VMS basic users.

With the standard AD users or local Windows users, the AD or the local Windows computer can be queried for groups and users, that then can be selected and added to the roles in question. With XProtect VMS basic users, the basic user can be manually created directly in the XProtect VMS and added to the roles.

When using external IDPs, the XProtect VMS cannot query the external IDP to read groups or users. Instead, the XProtect VMS automatically creates the external IDP users in the XProtect VMS and link them to roles based on claims provided to the users by the external IDP. Alternatively, in cases where claims related to the XProtect VMS roles are not provided to the external IDP users, the external IDP users are created in the XProtect VMS upon their first login, but they are not linked to any of the roles. The XProtect VMS administrator must manually add these users to the roles.

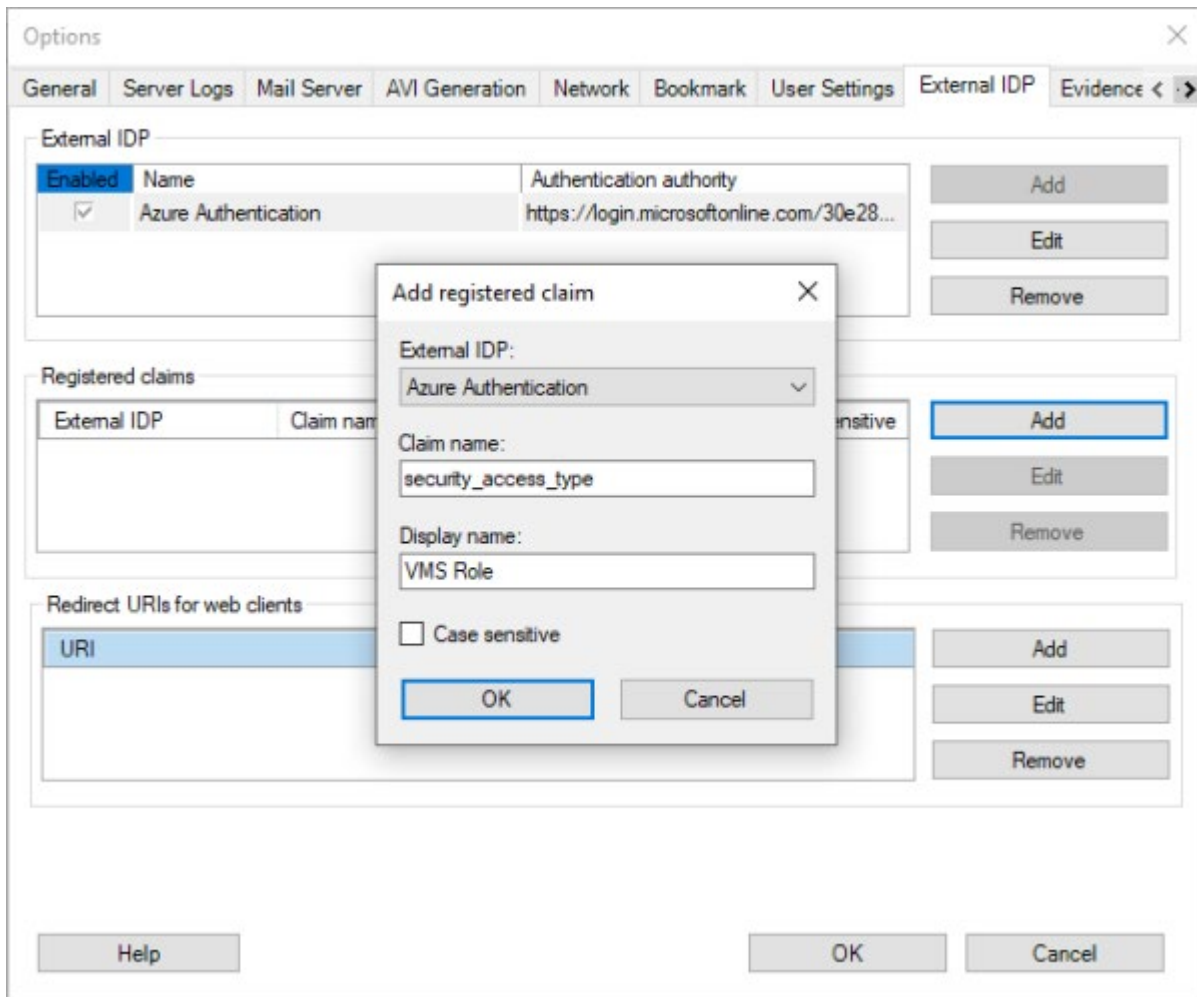
Claim-based XProtect VMS role linking

To automatically link the external IDP users to the XProtect VMS roles, the external IDP users must have XProtect VMS role-related claims defined. These claims are included in the users' ID token from the external IDP and are then used to link the external IDP users to the defined XProtect VMS roles.

To understand how external IDP claims can be used to link the external IDP users to the roles, it is important to know that the external IDP claims consist of a claim name and a value. For example:

- Claim name = "security_access_type"
- Claim value = "operator" (or = "admin", or = "guard", etc.)

To configure the XProtect VMS with the claims to look for and parse, the claims must be registered for the external IDP provider. This is done in the dialog where the external IDP is also defined.

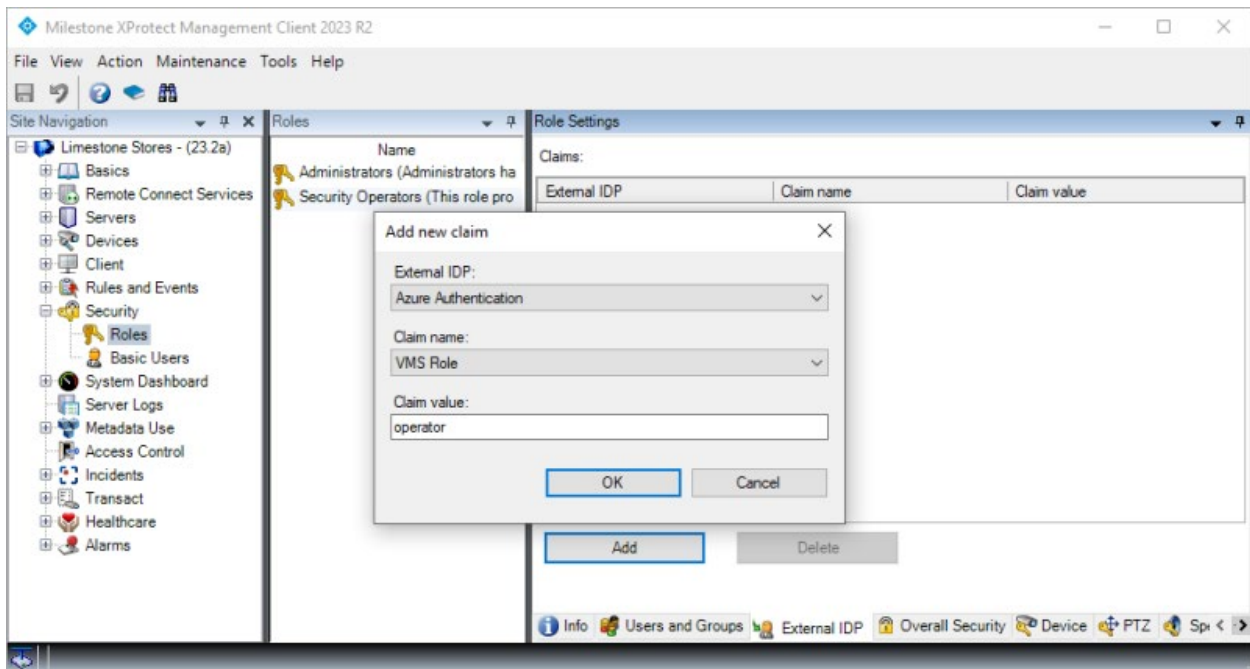


When registering a claim in the XProtect VMS, the claim name defined in the external IDP must be entered exactly as defined in the external IDP. Secondly, a display name for the claim to be used in the XProtect VMS roles dialog must also be entered.

For example, as shown in the screenshot.

- 'Claim name' = "security_access_type" (As defined in the external IDP)
- 'Display name' = "VMS Role" (For usage in the XProtect VMS roles)

The XProtect VMS will now parse the users' ID token. If their claim value matches the ones set for the roles, the external IDP users are linked to the XProtect VMS roles.



The next step is to configure the claim(s) and value(s) that should link the external IDP user to the individual XProtect VMS roles. This is done by selecting a role, and on the 'External IDP' tab, add claims.

In the dialog's 'Claim name' field, select what registered claim to parse. Then enter the claim value that will be used to link users to this role.

The use of the claims and their values in the roles is very flexible. When using claims and values in the roles, it is, for example, possible to:

- Use multiple claims in a single role using the same claim name, but with different values
- Use multiple claims in a single role using different claim names and values
- Use the same claims in multiple roles using the same claim name and values
- Use the same claims in multiple roles using the same claim name and different values for each role

When external IDP users log in to the XProtect VMS and they have claims with values that are linked to several roles, the user will get access to the sum of the roles just as if they were added manually to multiple roles.

One thing that isn't supported, though, is to use the logical "and" and "not" functions to link the external IDP user to the roles only if multiple conditions are true. For example, it is not possible to do the following:

- Link external IDP users to a role only when a user has two specific claims ("and" function)
- Reject linking the external IDP users to a role even though they have an appropriate claim, but in addition have a claim that is not allowed ("not" function).

If this kind of functionality is desired, the claims must be configured in the external IDP to provide a single claim with values that represent the result of the desired logical function for the specific external IDP users.

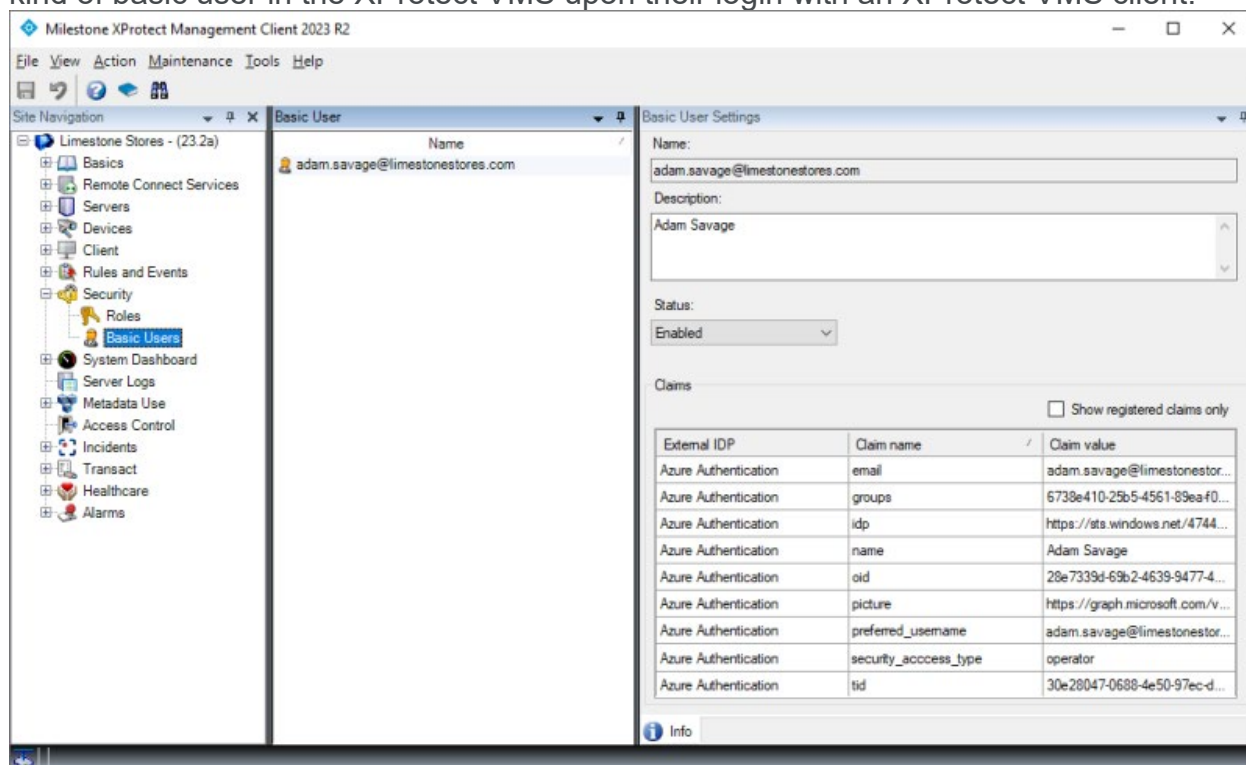
External IDP users in the XProtect VMS

With claims configured both in the external IDP and added to the XProtect VMS roles, the external IDP users will be created automatically in the XProtect VMS when the users are

authenticated by the external IDP, and they will have access per the roles they are linked to through their claims.

However, since the external IDP users are linked to the XProtect VMS roles through their claims, the external IDP users are not added to and listed in the specific roles – even if they technically have permissions for the roles per their claims. This is similar to how Microsoft AD users that are members of an AD group are not listed in the role when the AD group is added to a role.

However, unlike the users in AD groups, the external IDP users are auto-provisioned as a kind of basic user in the XProtect VMS upon their login with an XProtect VMS client.



Selecting an external IDP user will provide access to viewing the claims for the user (the ones provided at the latest log in).

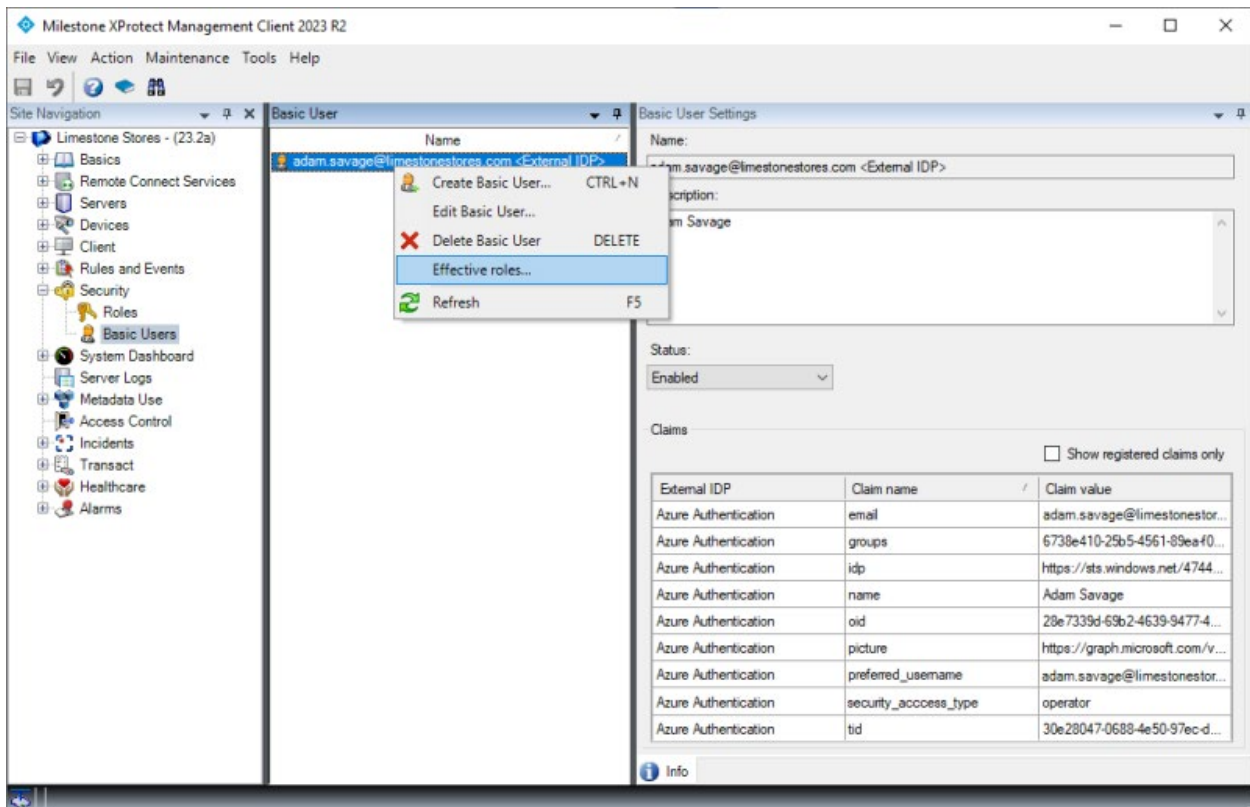
Furthermore, if required, the external IDP user can be disabled in the XProtect VMS even though the user is still enabled in the external IDP. This is done by changing the 'Status' from 'Enabled' to 'Locked out'.

Normally, a user could just be deleted. However, since the users are automatically created when authenticated by the external IDP, this wouldn't work for external IDP users.

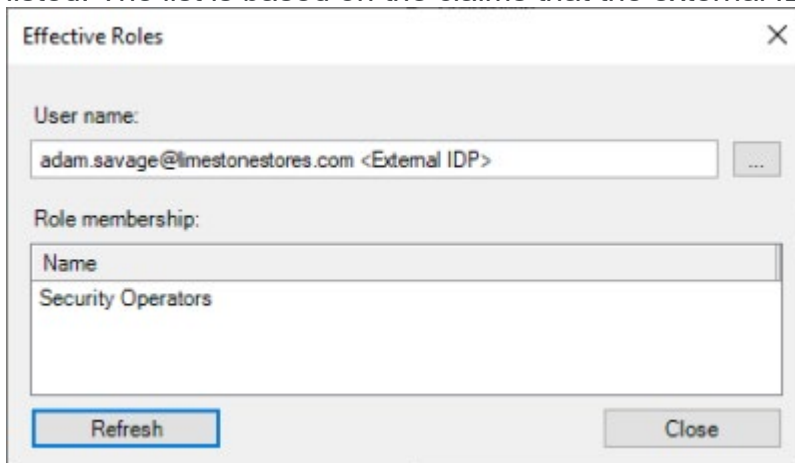
Effective roles

Since external IDP users that get their permissions based on claims are not added and listed in the roles, the information shown in the roles cannot be used to get an overview of which roles the external IDP users are linked to.

This information can, however, be obtained with the effective roles function. The function are available by right-clicking the external IDP user in the basic users list and selecting 'Effective roles...'



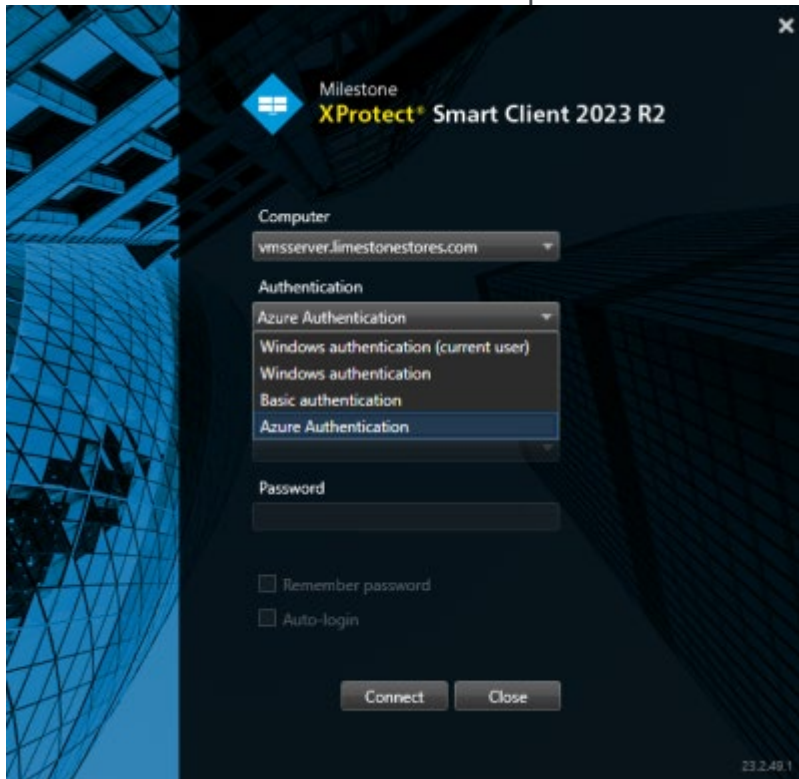
Doing so will open a dialog where the roles that the external IDP user is linked to are listed. The list is based on the claims that the external IDP user had at the latest log in.



Client experience

XProtect Smart Client and Management Client

With the external IDP properly configured, the XProtect Clients will support the external IDP as an additional authentication option.



The external IDP authentication option will only be shown when a computer address has been entered that points to an XProtect VMS with an external IDP configured.

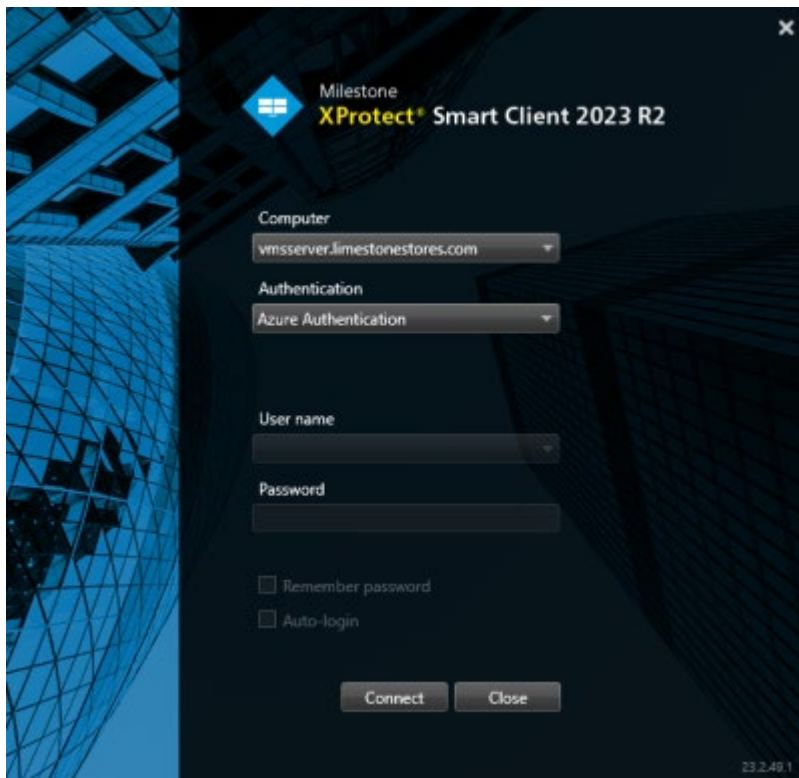
The client knows when to show the external IDP authentication option based on an API call to the entered address. The call queries which authentication options this XProtect VMS installation supports. The API call is made when the client is started and whenever the address is changed.

The particular API that the client queries is a public API that does not require any user authentication so this information can always be read by the client.

In case an incorrect address is entered, and the client thus doesn't get an answer to the API call, the client just defaults back to listing the standard authentication options.

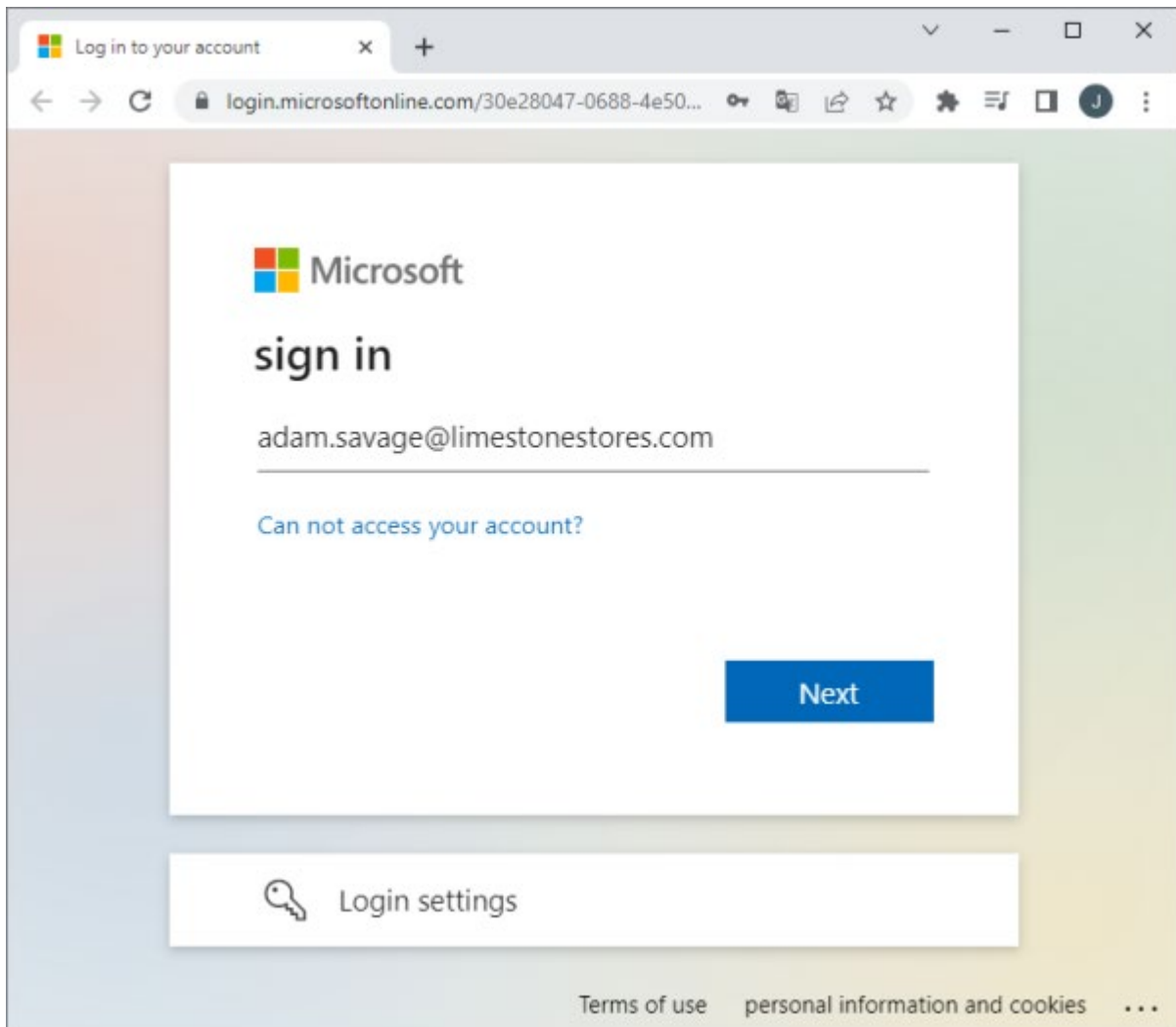
External IDP authentication

Note: In this white paper, Microsoft Entra ID (Azure) is used to illustrate the external IDP authentication dialogs and flow. Other IDP vendors may use a different terminology and authentication flow.

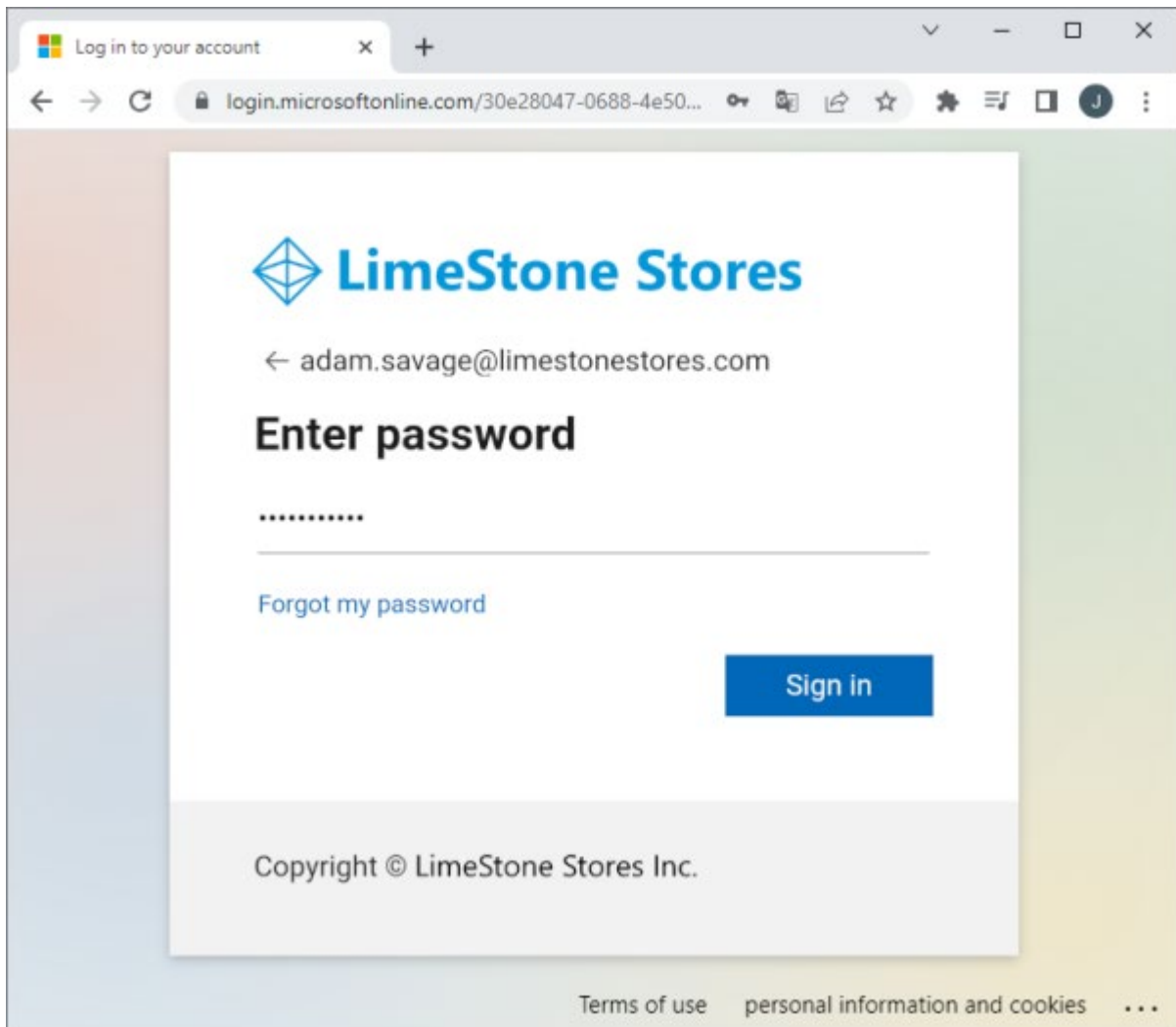


Having entered the address of the XProtect VMS computer and selected to authenticate using the external IDP, the 'User name' and 'Password' fields are disabled since this information must be provided from a browser showing the external IDP authentication page. Clicking 'Connect' will open a browser and show the external IDP's authentication page – called "sign in" for Microsoft Entra ID.

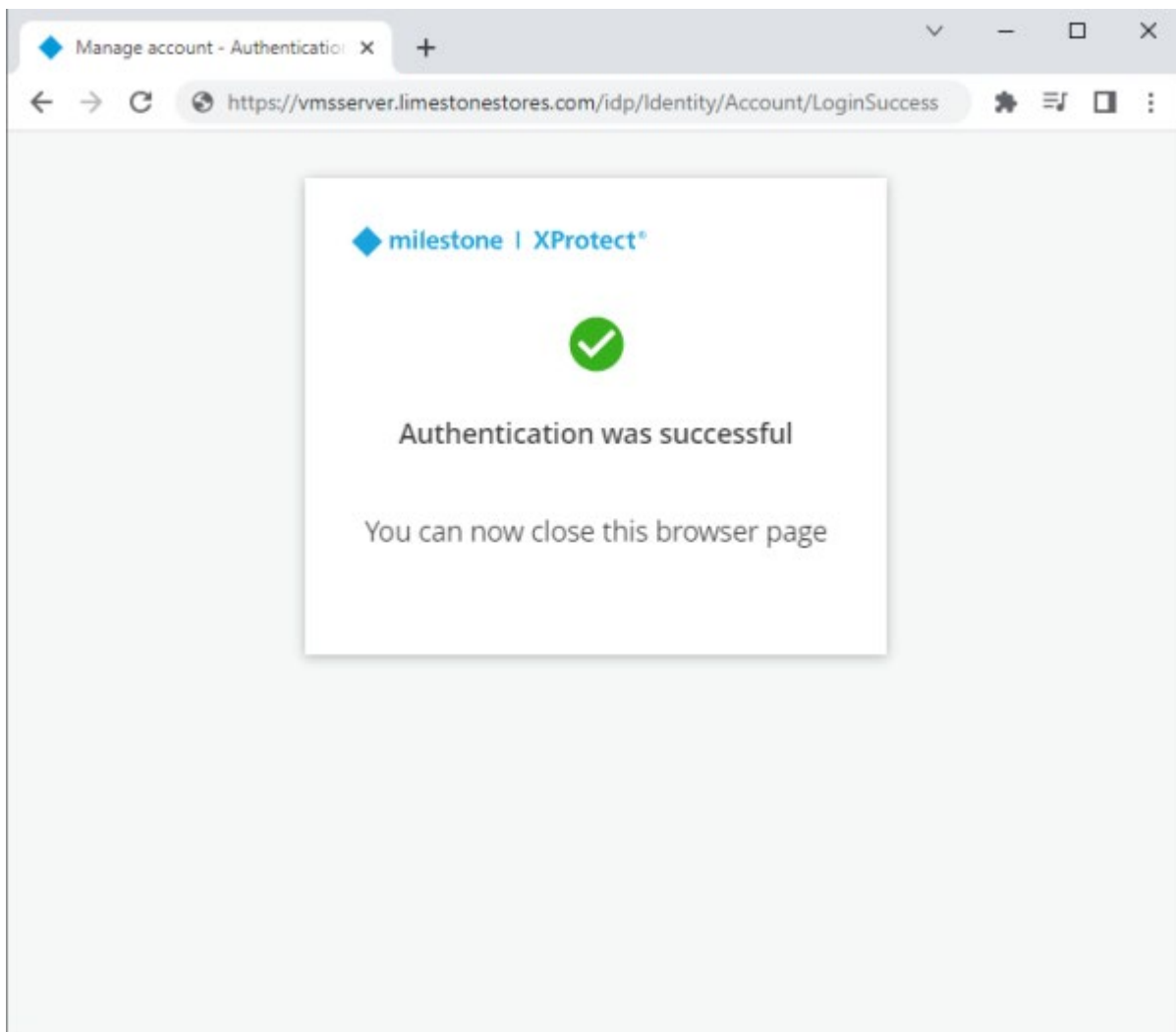
On the sign in page shown, the user enters his or her email address, and clicks 'Next'



Then, the user enters his or her password and clicks 'Sign in'.



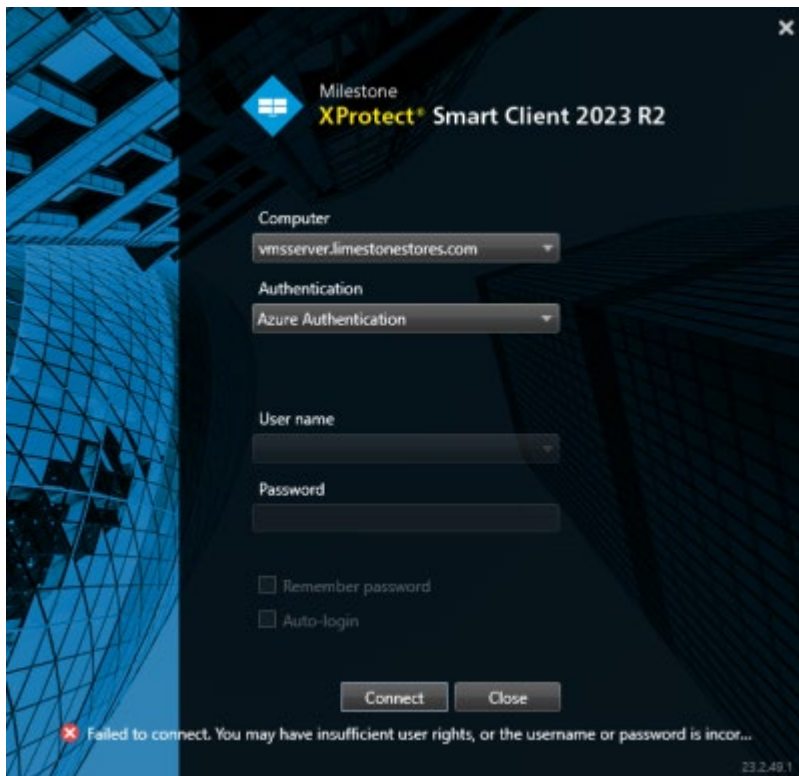
If the user authentication is successful, the web page states this, and the user can close the browser.



The XProtect VMS client will then automatically continue the regular login process and finally show the client.

No Claims, or claims not added to roles

It is still possible to use external IDP users in the XProtect VMS even if the external IDP users do not have claims defined for them that can be used by the XProtect VMS, or if the claims have not been configured in the XProtect VMS. This will just require one more configuration step in the process where the XProtect VMS administrator must manually add the external IDP user to one or more roles after the external IDP user's initial log in.



When this is the case, and an external IDP user attempts the initial log in to the XProtect VMS with one of the XProtect clients, the log in fails even after the external IDP user has been successfully authenticated by the external IDP.

The reason why the log in to the XProtect VMS fails even when the external IDP user is successfully authenticated by the external IDP, is that the user cannot be linked to any roles and thus does not have any permissions.

However, the user's act of attempting to log in to the XProtect VMS and successfully being authenticated by the external IDP, creates the external IDP user in the XProtect VMS as a kind of basic user.

When this has happened, the XProtect VMS administrator can manually add the external IDP user to one or more roles. The next time the external IDP user logs in, the XProtect VMS knows which role(s) the user belongs to and will allow log in and grant access to the allowed functions and resources.

Recommendation:

It is recommended to define XProtect VMS claims for the external IDP users and to configure the roles to link the external IDP users to these roles. This is recommended because the user experience for both the regular XProtect VMS users and the XProtect VMS' administrator is less than optimal when claims are not used, and because using claim-based linking to roles allows for effective, centralized user and permission management in the external IDP,

This will provide a smooth user experience in the XProtect VMS, and provide efficient and simple XProtect VMS role management in the external IDP.

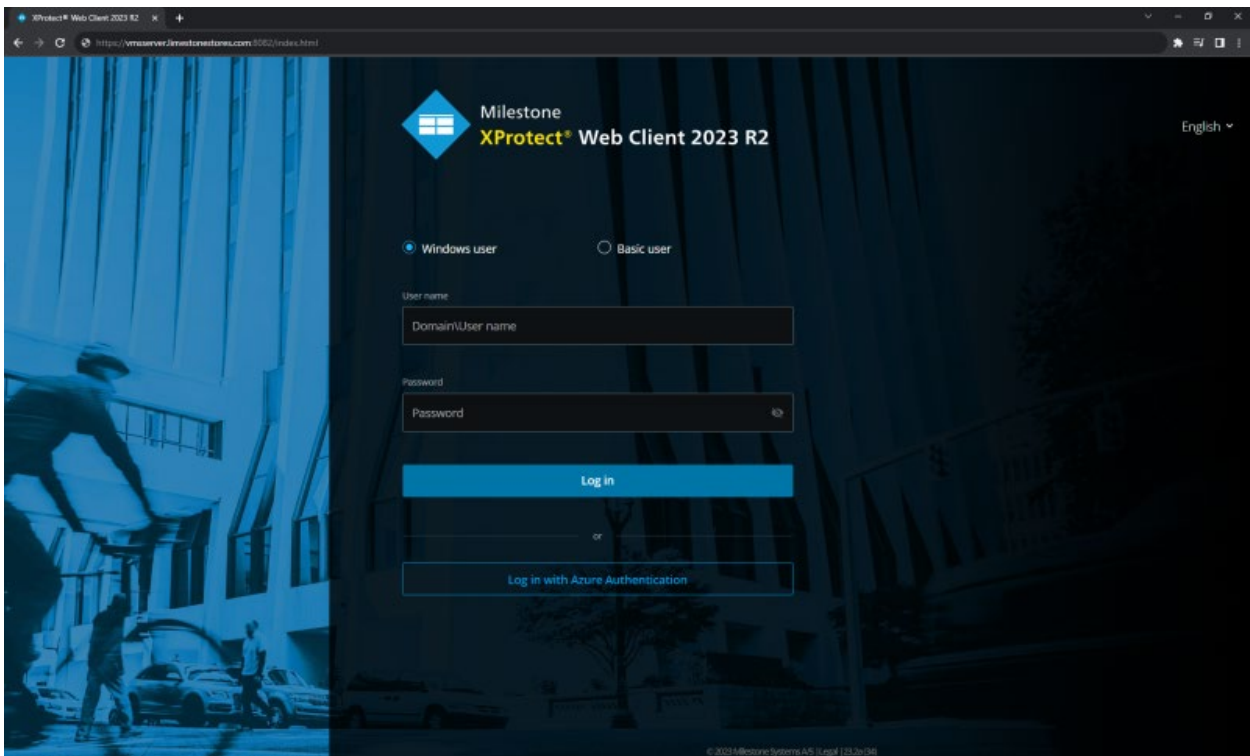
XProtect Web Client and Mobile client

To allow the XProtect Web Client and XProtect Mobile client to log in using the external IDP, a redirect URI address needs to be configured for the external IDP.

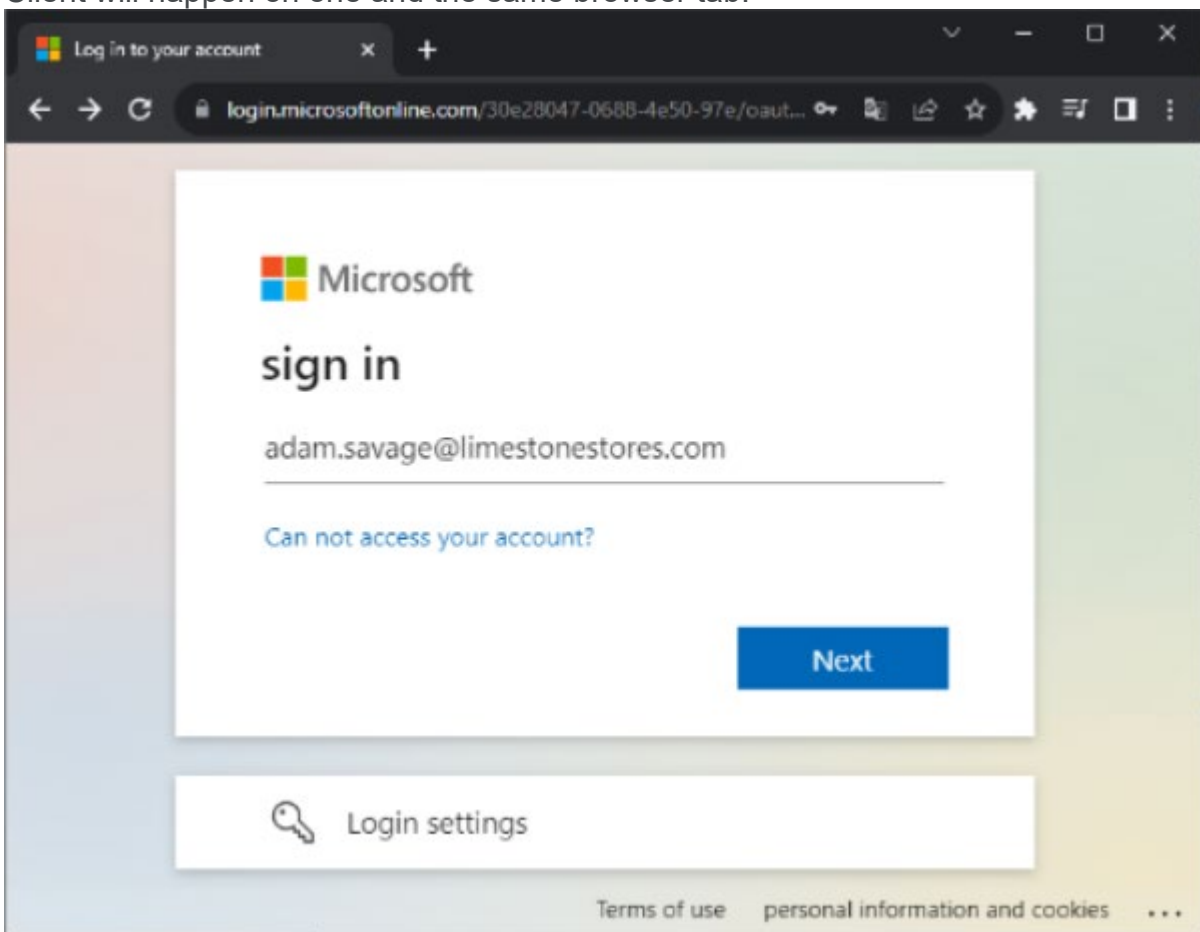
This is done in the dialog where the details of the external IDP are also defined. The URI must point to the Mobile Server address and include the port and “/index.html”. For example, “https://vmsserver.limestonestores.com:8082/index.html”

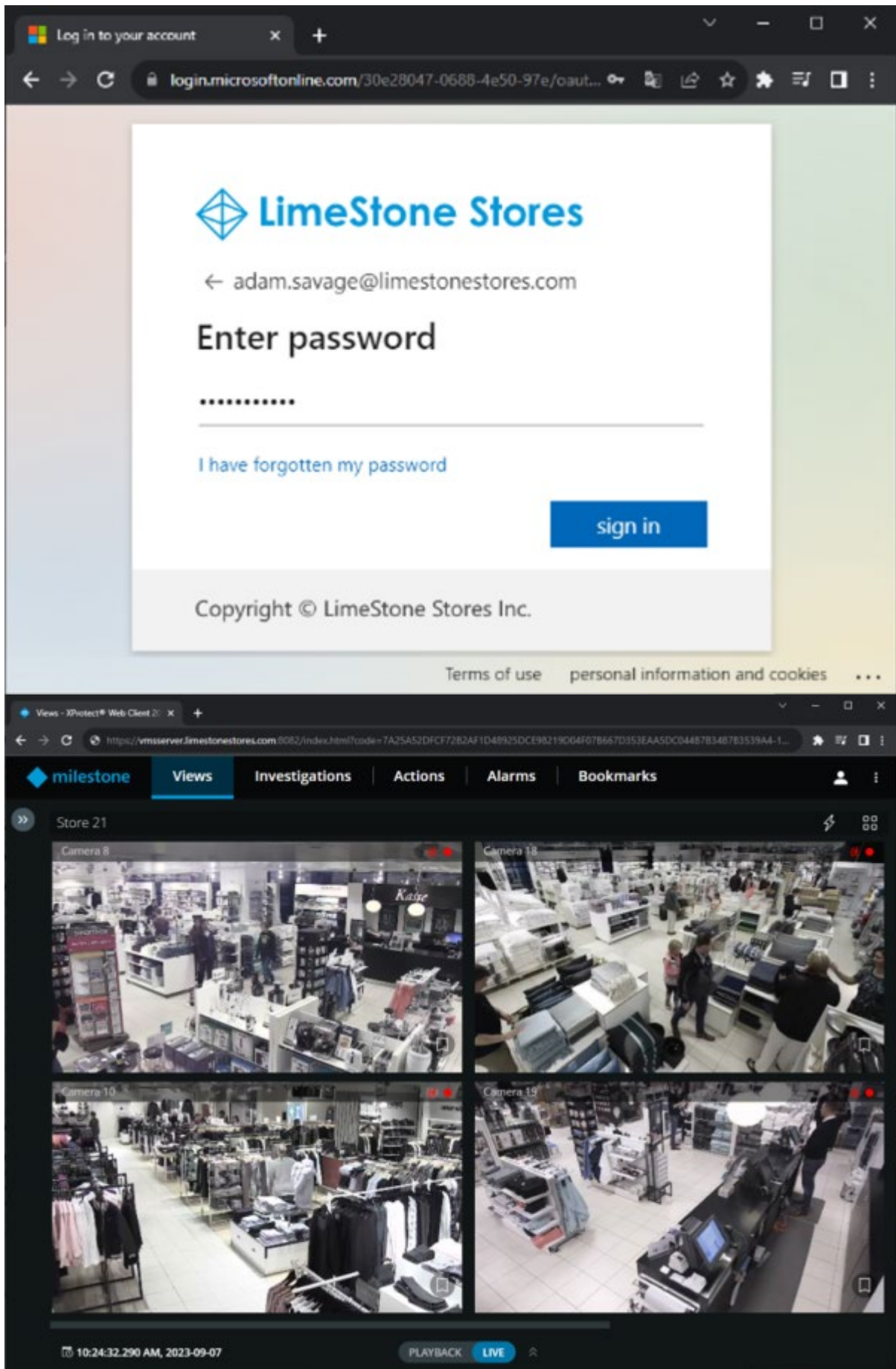
The screenshot shows the 'Options' dialog box with the 'External IDP' tab selected. The 'External IDP' section has a table with columns 'Enabled', 'Name', and 'Authentication authority'. The first row is 'Azure Authentication' with a checked 'Enabled' checkbox and the authentication authority 'https://login.microsoftonline.com/30e28...'. To the right of this table are 'Add', 'Edit', and 'Remove' buttons. Below this is the 'Registered claims' section with a table for 'External IDP' and 'Add', 'Edit', and 'Remove' buttons. The 'Redirect URIs for web' section has a table with columns 'URI' and 'Add', 'Edit', and 'Remove' buttons. The first row in this table has the URI 'https://vmsserver.limestonestores.com:8082/index.html'. The 'Edit' button for this row is highlighted. An 'Edit redirect URI' dialog box is open in the foreground, showing the URI 'https://vmsserver.limestonestores.com:8082/index.html' in a text field, with 'OK' and 'Cancel' buttons at the bottom. At the bottom of the 'Options' dialog are 'Help', 'OK', and 'Cancel' buttons.

With the redirect URI defined, users of the XProtect Web Client and XProtect Mobile client can also log in using the external IDP.
XProtect Web Client



Clicking the 'Log in with Azure Authentication' on the XProtect Web Client login page will launch the same browser authentication flow as for the XProtect Smart Client and XProtect Management Client. The only difference is that the log-in process with the XProtect Web Client will happen on one and the same browser tab.





XProtect Mobile Client

XProtect Mobile client

Adding the VMS server in the XProtect Mobile client, is done as usual by entering the address and port number for the Mobile Server.

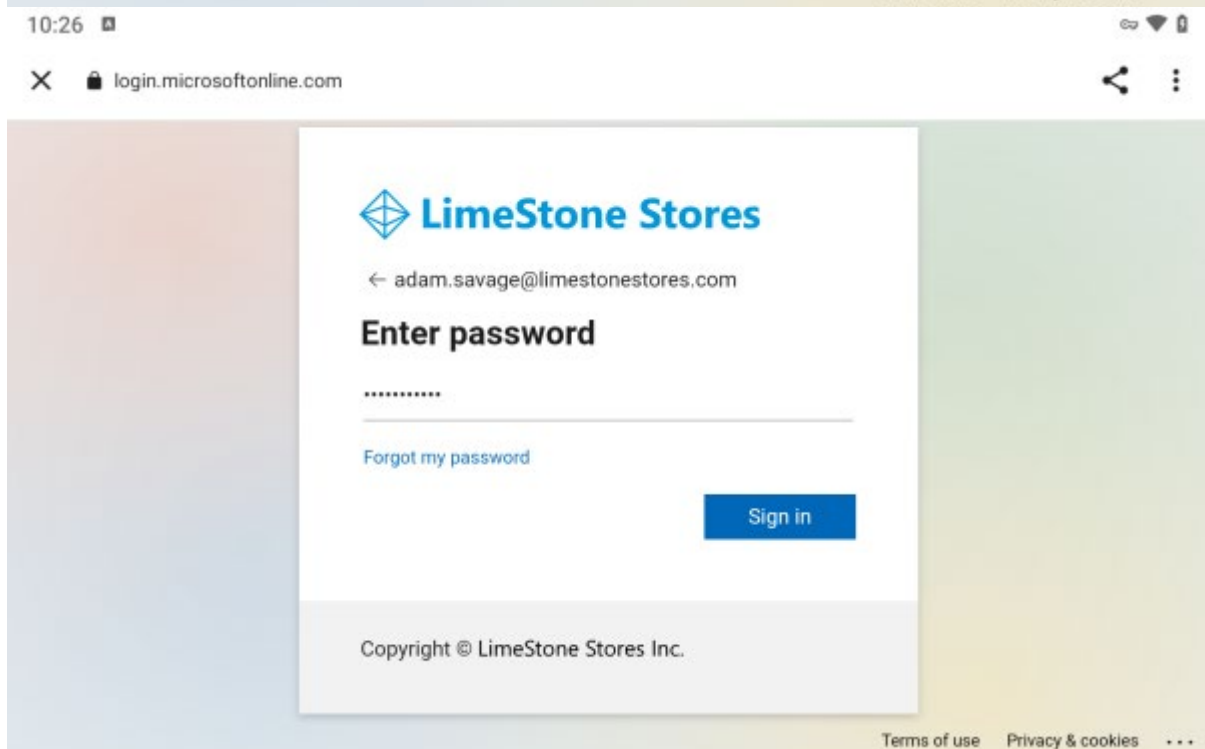
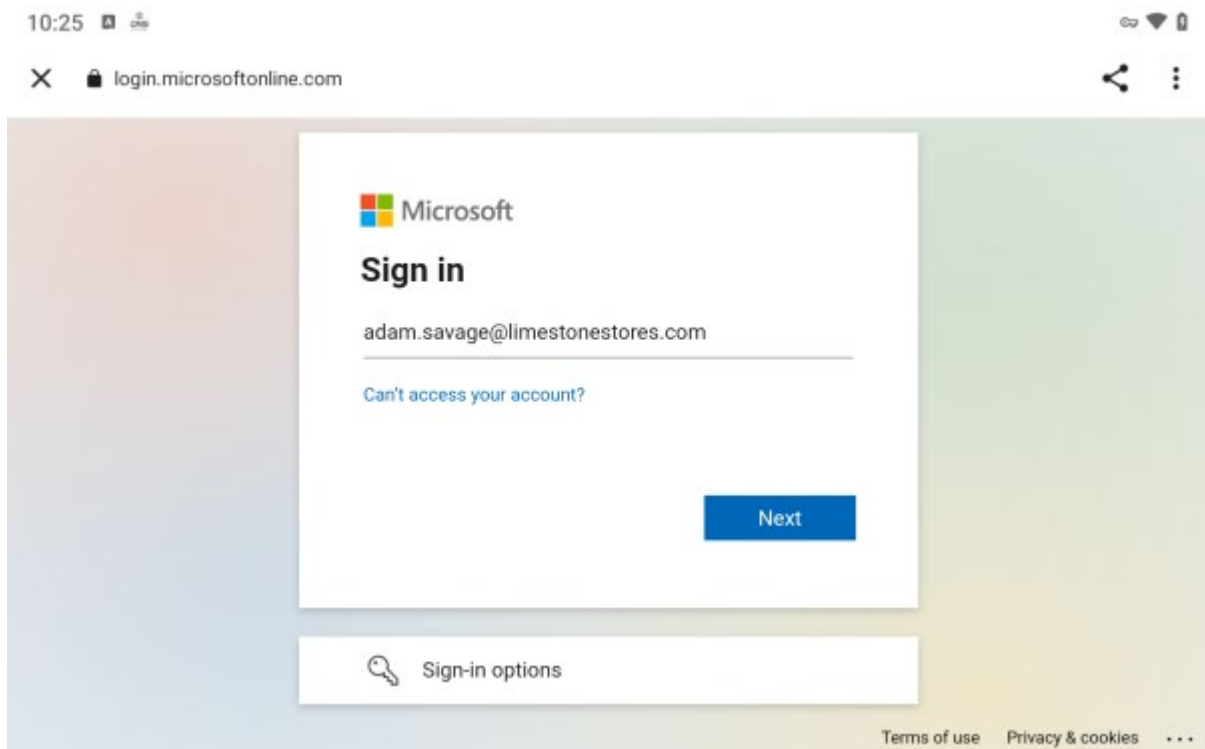
When the VMS server has been added, clicking the 'CONTINUE LOGIN' button will display the external IDP log in option in addition to the regular Windows user and Basic user log-in options.

The image displays two screenshots of the XProtect Mobile Client application interface.

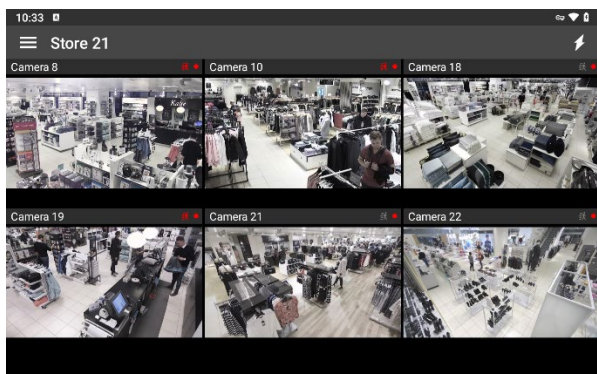
The top screenshot shows the 'Add server' screen. It features a dark blue header with a close button (X) and the title 'Add server'. Below the header, there are four input fields: 'Server name' (containing 'Limestone Stores Mobile Server'), 'Address' (containing 'vmsserver.limestonestores.com'), 'Protocol' (a dropdown menu showing 'https://'), and 'Port number' (containing '8082'). At the bottom, there are two buttons: a large blue 'CONTINUE LOGIN >' button and a smaller 'SAVE AND LOG IN LATER' button.

The bottom screenshot shows the 'Login' screen. It features a dark blue header with a back arrow and the title 'Login'. Below the header, there are two radio buttons: 'Windows user' (selected) and 'Basic user'. Below the radio buttons, there are two input fields: 'User name' and 'Password' (with a toggle icon). Below the input fields, there is a 'Remember me' toggle switch (turned on). At the bottom, there are two buttons: a large blue 'LOG IN' button and a smaller 'LOG IN WITH AZURE AUTHENTICATION' button.

Clicking the 'LOG IN WITH AZURE AUTHENTICATION' button will open a browser page and provide access to the regular authentication flow on the external IDP.



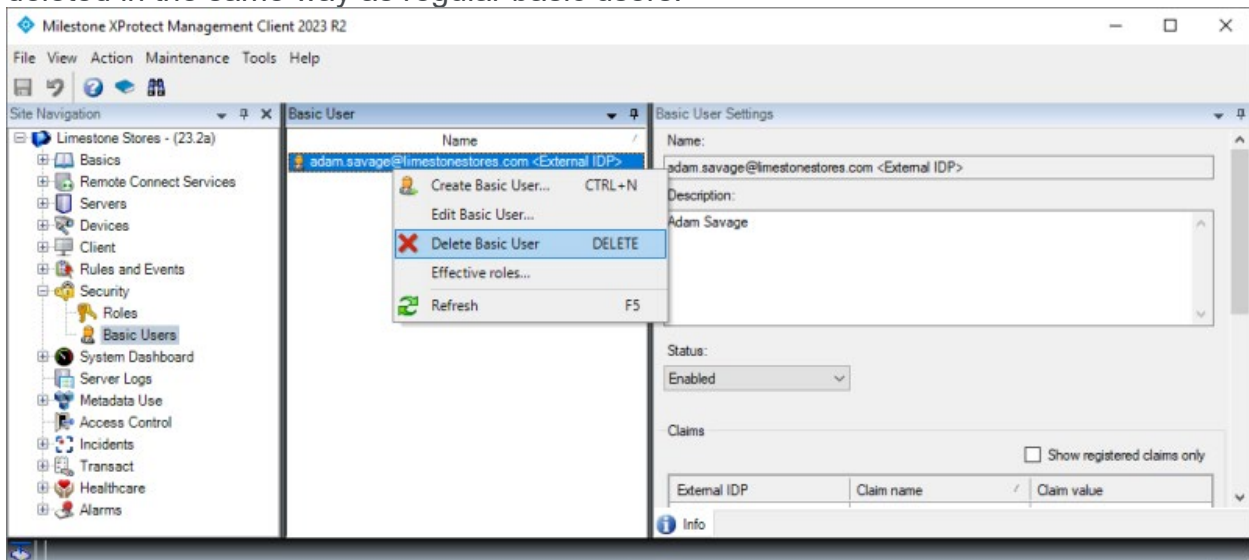
When log in has been completed, the XProtect Mobile client is displayed and can be used. One thing to note when using the XProtect Mobile client with an external IDP login is that the client credentials cannot be saved. The user must always authenticate with the external IDP to use the client.



User management and audit logs

Deleting and disabling external IDP users

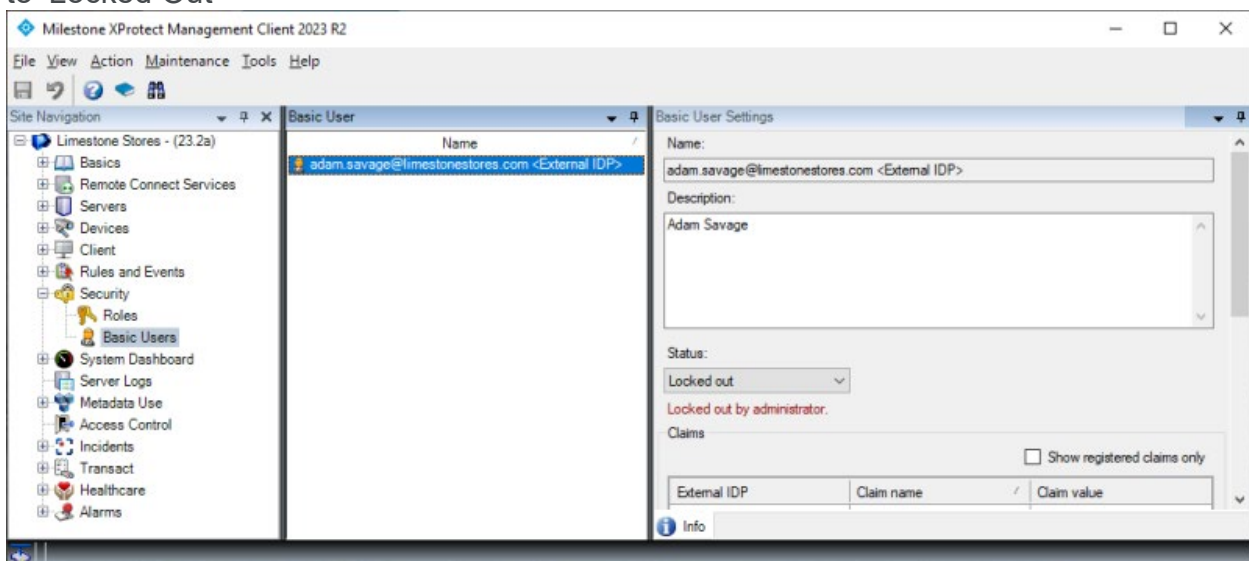
External IDP users are listed along with the basic users, and the external IDP users can be deleted in the same way as regular basic users.



However, as long as the external IDP is still configured in the XProtect VMS and the external IDP user is still enabled in the external IDP, it will not have any effect to delete an external IDP user.

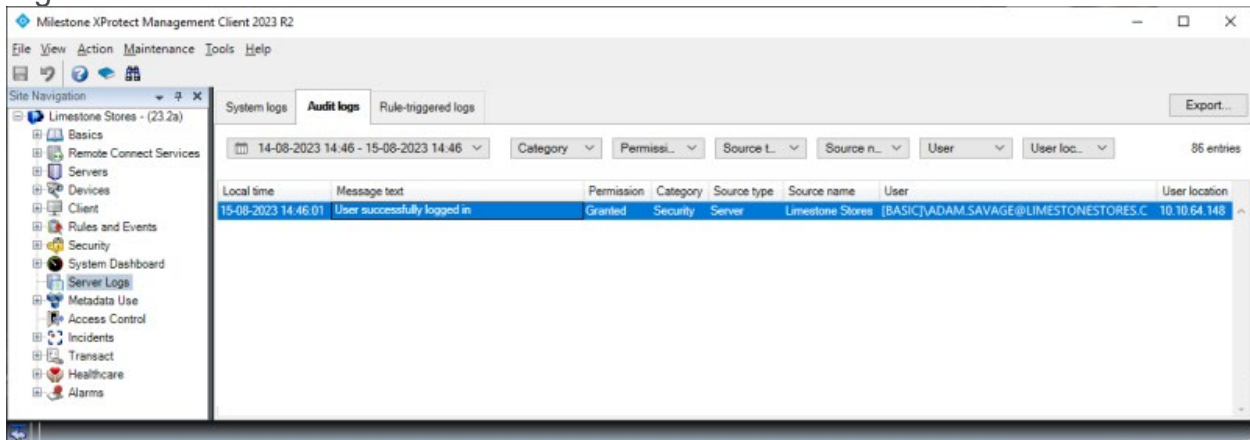
The external IDP user will simply be added automatically again the next time the user logs in to the XProtect VMS.

If it is necessary to block an external IDP user from logging in to the XProtect VMS while the user still exists and is enabled in the external IDP, the external IDP user can be blocked from logging in to the XProtect VMS by changing the user's status from 'Enabled' to 'Locked Out'



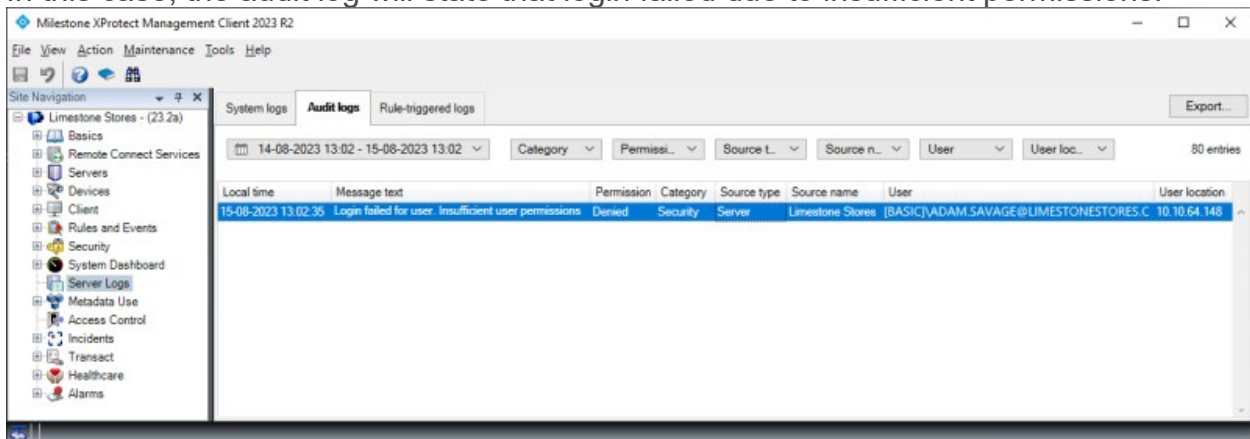
Audit logs

The audit logs added for actions done by the external IDP users are the same as for the regular Windows AD or basic users.



Even though claims have not been configured for the external IDP users or added to the XProtect VMS roles, and an external user has not yet been manually added to a role, this user will still be able to authenticate towards the external IDP. However, the XProtect VMS will deny access, because the user is not a member of a role or linked to a role via the claims and thus does not have any permissions for the XProtect VMS.

In this case, the audit log will state that login failed due to insufficient permissions.



External IDP user limitations

Milestone Federated Architecture

Milestone XProtect VMS supports a Milestone Federated Architecture setup with an option to use an external IDP to log in from sites within the federated hierarchy. This allows users of XProtect Smart Client to log in from a federated site via an external IDP. XProtect Smart Client and the VMS on the main and sub-sites must be version 2024 R2 or newer. Refer to this Knowledge Base article for information on how to set up an external IDP to log in from sites within the federated hierarchy: [How to set up External IDP in a Milestone Federated Architecture](#).

For more information: [White Paper - Milestone Federated Architecture](#).

Milestone Interconnect

When attaching a remote XProtect VMS site to a central XProtect Corporate installation via Milestone Interconnect, the authentication towards the remote XProtect site must be done using Microsoft AD users, Windows users or basic users. External IDP users cannot be used for interconnecting remote XProtect sites.

For more information: [White paper - Milestone Interconnect](#)

Benefits and summary

Organizations using a plethora of applications, services and products that are accessed across multiple platforms like PCs, MACs, Smart Phones and browsers, need a way to provide their users with a unified way to log in regardless of platform, service, or product used.

For this, managing users in a regular on-premises Microsoft Active Directory (AD) will not suffice because the AD often is not supported by all the products, services, or interfaces used. Instead, an Identity Provider supporting standard authentication protocols and Single sign-on (SSO) is used.

The Identity Provider has all the functionality that is required to manage users and enable cross-platform SSO authentication. Furthermore, with support for so-called claims, the Identity Provider can also provide functionality for managing the users' permissions for the various products and services used within the organization.

When the need for a video surveillance product arises for organizations that use an Identity Provider to manage their users, the obvious choice would be to select a video surveillance product that can be integrated with their chosen Identity Provider. Since all Milestone XProtect VMS products and clients support SSO integration with Identity Providers supporting [OpenID Connect \(OIDC\)](#) and [OAuth2](#), the Milestone XProtect VMS is a safe choice for any organization.

Furthermore, with an external IDP, claims supported by the Identity Provider, and support for claim-based VMS role linking in the XProtect VMS product it becomes very easy and efficient to manage the organizations users and centrally control permissions across various products and services, including the XProtect VMS.

User-management tasks like creating and deleting users and editing access permissions for the XProtect VMS is as simple as just creating a user in the Identity Provider and setting a VMS-role related claim for the user. The user can then immediately log in and access the XProtect VMS without having to be manually added or having to change the XProtect VMS role settings. The same applies for removing or changing user access to the XProtect VMS. Users simply get access to the XProtect VMS per their configuration in the Identity Provider.

Organizations using an XProtect VMS product that is integrated with an Identity Provider, will get a very efficient and simple solution for managing their users and permissions thought their organization regardless of the application, service, interfaces and what XProtect VMS surveillance solution they use.



About Milestone Systems

Milestone Systems is a leading provider of data-driven video technology software in and beyond security that helps the world see how to ensure safety, protect assets, and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 500,000 customer sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.

www.milestonesystems.com