Authentification unique (SSO) Microsoft Office 365 avec AD FS 2.0

Microsoft France

Publication : Juin 2012

Version : 1.0a

Auteurs : Philippe Beraud (Microsoft France), Jean-Yves Grasset (Microsoft France)
Collaborateur : Philippe Maurent (Microsoft Corporation)

Résumé

Bien qu'ils prennent en charge les protocoles WS-Federation (WS-Fed) et WS-Trust, les services AD FS (Microsoft Active Directory Federation Services) 2.0 fournissent une authentification unique (également appelée fédération des identités) basée sur les revendications (Web) avec Microsoft Office 365 et son application web et ses applications clientes riches.

Basé sur la documentation existante, ce document est conçu pour fournir une meilleure compréhension des différentes options de déploiement de l'authentification unique pour les services dans les services dans Office 365, pour expliquer comment activer l'authentification unique à l'aide des informations d'identification Active Directory d'entreprise et d'AD FS 2.0 à utiliser dans Office, et les différents éléments de configuration qu'il faut connaître pour un tel déploiement.

Ce document est conçu pour les architectes système et les informaticiens qui veulent comprendre les éléments fondamentaux de la fonctionnalité d'authentification unique d'Office 365 avec AD FS 2.0, ainsi que la planification et le déploiement dans leur environnement.

Microsoft

Contenu

1 Introduction

Microsoft Office 365[1] fournit un accès sécurisé où que vous soyez à la messagerie professionnelle, aux calendriers partagés, à la messagerie instantanée, aux conférences vidéo et à la collaboration sur des documents.

Il correspond à la version sur le nuage des produits de communication et de collaboration de Microsoft intégrant la version la plus récente de la suite de bureau Microsoft pour les entreprises de toutes tailles. Office 365 comprend :

- **Microsoft Office** : Microsoft Office Professionnel Plus 2010 se connecte de façon transparente à Microsoft Office Web Apps pour une meilleure productivité entre les PC, les appareils mobiles et les navigateurs ;

> **Remarque :**
>
> *Un appareil compatible, une connexion Internet et un navigateur pris en charge sont requis. Certaines fonctionnalités mobiles nécessitent Office Mobile 2010, qui n'est pas fourni avec les applications ou les suites Office 2010, ni avec Office Web Apps. De plus, certaines différences de fonctionnalités existent entre Office Web Apps, Office Mobile 2010 et les applications Office 2010.*

- **Microsoft Exchange Online** : Exchange Online propose la messagerie, le calendrier et les contacts sur le nuage avec des solutions antivirus et anti-spam les plus récentes. Il permet d'accéder à la messagerie sur n'importe quel appareil mobile et tire parti des options de la messagerie vocale, de la messagerie unifié et de l'archivage ;
- **Microsoft SharePoint Online** : SharePoint Online est un service sur le nuage qui permet de créer des sites pour la collaboration entre collègues, partenaires et clients à l'aide des réseaux sociaux et de la personnalisation ;
- **Microsoft Lync Online** : Lync Online propose des fonctionnalités de réunion en ligne, de présence et de messagerie instantanée sur le nuage avec partage d'écran, et conférence audio et vidéo.

> **Remarque :**
>
> *Pour obtenir des informations supplémentaires sur Office 365 en plus du contenu de ce document, voir la documentation en ligne du produit (éventuellement en anglais)[2], le guide de déploiement Office 365 pour les entreprises (éventuellement en anglais)[3], le site web TechCenter Office 365[4], et le site web de la communauté Office 365 (blogs, forums, wikis, etc.)[5].*

À l'exception des sites Internet pour les accès anonymes créés avec SharePoint Online, les utilisateurs doivent être authentifiés pour accéder aux services dans Office 365.

---

[1] Microsoft Office 365 : http://office365.microsoft.com/

[2] AIDE D'OFFICE 365 : http://onlinehelp.microsoft.com/en-us/office365-enterprises/

[3] GUIDE DE DEPLOIEMENT OFFICE 365 POUR LES ENTREPRISES : http://www.microsoft.com/download/en/details.aspx?id=26509

[4] Site web TechCenter Office 365 : http://technet.microsoft.com/fr-fr/office365/default

[5] Site web de la communauté Office 365: http://community.office365.com/fr-fr/default.aspx

1.1 Objectifs de ce document

Par l'intermédiaire de sa fonctionnalité d'authentification unique, Office 365 permet aux organisations une authentification avec les services Active Directory Domain Services (AD DS) de l'organisation, ce qui permet aux utilisateurs d'utiliser leurs informations d'identification d'entreprise pour accéder aux services d'Office 365 pour lesquels ils ont été configurés.

Ainsi, les utilisateurs qui se trouvent sur le réseau d'entreprise interne ou qui sont connectés via un réseau VPN ont un accès transparent aux services dans Office 365. Si les utilisateurs accèdent aux services dans Office 365 de chez eux ou d'un ordinateur qui n'est pas connecté au réseau d'entreprise, ils auront toujours accès aux services d'Office 365 à l'aide de leurs informations d'authentification d'entreprise. Une telle expérience de connexion des utilisateurs était attendue par de nombreuses organisations :

- **Ordinateur de travail sur un réseau d'entreprise** : quand les utilisateurs sont au bureau et connectés au réseau d'entreprise, l'authentification unique leur permet d'accéder aux services dans Office 365 sans avoir besoin de se reconnecter ;
- **Itinérance avec un ordinateur de bureau** : pour les utilisateurs qui ont ouvert une session sur des ordinateurs joints à un domaine avec leurs informations d'identification d'entreprise, mais qui ne sont pas connectés au réseau d'entreprise (par exemple, un ordinateur de bureau chez vous ou dans un hôtel), l'authentification unique leur permet d'accéder aux services d'Office 365 sans avoir besoin de se reconnecter ;
- **Ordinateur personnel ou public** : quand l'utilisateur utilise un ordinateur qui n'est pas joint au domaine d'entreprise, l'utilisateur doit se connecter avec les informations d'identification d'entreprise pour accéder aux services dans Office 365. Cela représente toujours un avantage, car les informations d'identification pour leur accès au réseau d'entreprise et à Office 365 seront les mêmes.

Au moment de la rédaction de ce document, cette authentification avec la fonctionnalité d'identification unique d'Office 365 est fournie uniquement via le service Active Directory Federation Services (AD FS) 2.0 que l'organisation déploie localement et qui communique de façon sécurisée avec Office 365.

OASIS

Pour une brève introduction, consultez les normes OASIS telles que :

- WS-Federation (WS-Fed) (éventuellement en anglais)[6],
- WS-Trust (éventuellement en anglais)[7],
- Security Assertion Markup Language (SAML) 2.0 (éventuellement en anglais)[8],

Microsoft Active Directory Federation Services (AD FS) 2.0 Release to Web (RTW)[9][10] fournit l'authentification unique (également appelée fédération des identités) entre domaines (Web) basée sur les revendications avec les solutions de fédération Microsoft et non-Microsoft.

---

[6] WEB SERVICES FEDERATION LANGUAGE (WS-FEDERATION) VERSION 1.2 : http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf

[7] WS-TRUST VERSION 1.3 : http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf

[8] SECURITY ASSERTION MARKUP LANGUAGE (SAML) 2.0 : http://go.microsoft.com/fwlink/?LinkId=193996

[9] Téléchargement Microsoft AD FS 2.0 Release to Web (RTW) : http://www.microsoft.com/downloads/details.aspx?FamilyID=118c3588-9070-426a-b655-6cec0a92c10b

[10] Téléchargement Microsoft AD FS 2.0 : http://www.microsoft.com/downloads/details.aspx?FamilyID=118c3588-9070-426a-b655-6cec0a92c10b

Wikipedia (éventuellement en anglais)[11] définit la fédération ainsi :

> *« L'identité fédérée, ou la fédération des identités, décrit les technologies, normes et cas pratiques qui servent à activer la portabilité des informations d'identité entre des domaines de sécurité autonomes. L'objectif de la fédération des identités est de permettre aux utilisateurs d'un domaine d'accéder de façon sécurisée aux données et systèmes d'un autre domaine de façon transparente, sans administration utilisateur redondante. »*

Basé sur les articles de la base de connaissances et la documentation Microsoft existants, ce document présente plus en détail la fonctionnalité d'authentification unique (également appelée fédération des identités) d'Office 365.

Remerciements à Ross Adams, Microsoft Senior Program Manager, pour le contenu fourni sur ce sujet, tel que le webcast MSDN Channel 9 Microsoft Office 365: Identity and Access Solutions (éventuellement en anglais).[12]

Dans ce but, après une brève description de la technologie AD FS 2.0 pour présenter les concepts clés, la configuration requise et les composants pour l'ensemble de ce document, il :

- décrit les différentes options des identités dans Office 365 ;
- décrit rapidement dans ce contexte l'architecture et les fonctionnalités des identités dans Office 365 ;
- décrit différents scénarios d'implémentation pour l'authentification fédérée ;
- décrit le fonctionnement de l'authentification fédérée avec AD FS 2.0 ;
- propose des informations supplémentaires à connaître.

, afin que les projets Microsoft Office 365 qui utilisent AD FS 2.0 dans ce contexte puissent être exécutés plus facilement, et que les utilisateurs réalisent le potentiel de l'offre Microsoft Office 365.

Bien que l'authentification unique ne soit pas requise pour la synchronisation d'annuaires (mais permettra une expérience utilisateur plus riche), la synchronisation d'annuaires est cependant un élément requis pour l'authentification unique.

C'est pourquoi, l'implémentation de la synchronisation d'annuaires est nécessaire afin de conserver le service AD DS local synchronisé avec l'annuaire Microsoft Online Services. Cela permet le contrôle et la gestion du compte utilisateur d'entreprise de la façon traditionnelle, c'est-à-dire via Utilisateurs et ordinateurs Active Directory. Cet élément permet vraiment la gestion transparente des utilisateurs entre l'environnement local et l'environnement Office 365. L'outil de synchronisation d'annuaires Microsoft Online Services permet aux administrateurs de service de conserver les utilisateurs, les contacts et les groupes Office 365 à jour avec les modifications apportées au service local AD DS.

Il est recommandé d'installer et de configurer l'authentification unique, puis d'implémenter la synchronisation d'annuaires. Cela n'est pas une obligation, mais est fortement conseillé.

La synchronisation d'annuaires n'est pas une nouveauté d'Office 365. Elle est basée sur Microsoft Identity Lifecycle Management (ILM) 2007 (désormais Microsoft Forefront Identity Manager (FIM) 2010). La configuration de la synchronisation d'annuaires a été simplifiée pour l'environnement Office 365. Il n'existe pas de configuration manuelle compliquée, tout est configuré via des Assistants.

La synchronisation d'annuaires n'est pas approfondie dans ce document. Pour obtenir des détails sur ce sujet, voir SYNCHRONISATION ACTIVE DIRECTORY : FEUILLE DE ROUTE[13] et Gérer la synchronisation d'annuaires[14] dans la documentation en ligne d'Office 365.

---

[11] Définition de la fédération des identités de Wikipedia : http://en.wikipedia.org/wiki/Federated_identity

[12] MICROSOFT OFFICE 365: IDENTITY AND ACCESS SOLUTIONS: http://channel9.msdn.com/Events/TechEd/NorthAmerica/2011/OSP215

1.2 Objectifs de ce document

Pour couvrir les objectifs mentionnés, ce document adopte une organisation en fonction des thèmes suivants, chacun étant expliqué dans les sections suivantes :

- Présentation d'Active Directory Federation Services (AD FS) 2.0;
- Authentification fédérée dans Microsoft Office 365;
- Fonctionnement de l'authentification fédérée dans Office 365;
- Présentation de la configuration SSO et des éléments requis associés;
- Autres informations à prendre en compte;

Enfin, des références sont fournies dans les annexes pour permettre des recherches d'informations supplémentaires sur le web.

1.3 Public visé

L'authentification unique (entre domaines) − également appelée fédération des identités − est un large sujet, avec de nombreuses facettes, niveaux de compréhension, protocoles, normes, jetons, etc. Ce document s'intéresse à l'authentification unique dans le cadre d'Office 365 d'un point de vue conceptuel et technique.

Au moment de la rédaction de ce document, et comme indiqué précédemment, AD FS 2.0 est la seule technologie prise en charge qui fournit cette fonctionnalité (même si cela est amené à évoluer à l'avenir).

> **Remarque :**
>
> *Pour plus d'informations sur la fonctionnalité d'authentification unique d'Office 365 avec AD FS 2.0 en plus du contenu de ce document, voir la documentation du produit (éventuellement en anglais)[15], le Forum aux questions sur l'authentification unique (éventuellement en anglais)[16] dédié et le plan du site Authentification unique Office 365 (éventuellement en anglais)[17].*

Ce document est conçu pour les architectes système et les informaticiens qui souhaitent comprendre Office 365. Pour une introduction, voir la série d'ateliers virtuels sur Office 365 (éventuellement en anglais)[18] disponible sur le sujet.

---

[13] SYNCHRONISATION ACTIVE DIRECTORY : FEUILLE DE ROUTE : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/ff652543.aspx

[14] Gérer la synchronisation d'annuaires : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/ff652533.aspx

[15] Planifier et déployer Active Directory Federation Services 2.0 pour l'utilisation avec l'authentification unique : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/ff652539.aspx

[16] FORUM AUX QUESTIONS SUR L'AUTHENTIFICATION UNIQUE : http://community.office365.com/en-us/w/sso/295.aspx

[17] Plan du site authentification unique Office 365 : http://community.office365.com/en-us/w/sso/office-365-sso-content-map.aspx

[18] Ateliers virtuels Office 365 pour les professionnels de l'informatique : http://technet.microsoft.com/fr-fr/office365/hh699847

1.4 À propos de la démonstration live sur MTC Paris/Interop Lab

Microsoft Technology Center

Microsoft Technology Centers (éventuellement en anglais)[19] (MTC) sont des environnements de collaboration qui fournissent un accès à des technologies innovantes et des compétences d'experts, permettant à nos clients et partenaires de planifier, concevoir et déployer des solutions qui répondent à leurs besoins.

Depuis 2004, MTC Paris, fait partie des centres globaux conçus pour fournir à nos clients des procédures qui expliquent comment une solution Microsoft peut les aider à atteindre leurs objectifs d'entreprise clés. Dans ce centre, les architectes MTC et les experts des technologies Microsoft, via un processus de découverte et des démonstrations basées sur des scénarios s'exécutant dans le centre de données MTC, jouent un rôle crucial pour répondre aux défis de nos clients.

MTC Paris héberge et gère Microsoft France Interop Lab afin de permettre à nos clients de voir et de comprendre comment les solutions et actions Microsoft peuvent interagir avec d'autres technologies ou produits des domaines suivants : services web avancés, PHP, Java, SAP, gestion du cycle de vie des applications, et sécurité et identité.

Dans ce laboratoire, les clients et partenaires testent des configurations techniques de différents fabricants afin d'adapter leurs solutions à leurs besoins d'un point de vue de l'interopérabilité fonctionnelle. MTC Paris héberge plus de 20 solutions différentes. Ces solutions sont déployées sur l'infrastructure du centre de données MTC Paris qui se compose de plus de 300 serveurs et 200 téraoctets de stockage. Le travail avec des fabricants différents, permet de faciliter l'intégration de systèmes hétérogènes. L'interopérabilité devient une garantie de l'intégration pour nos clients, ce qui leur permet un retour sur investissement maximum en termes d'innovation.

Afin de garantir la portabilité des identités et la sécurité dans un environnement souple, il est fondamental de maîtriser la gestion des identités dans chacun des domaines de sécurité utilisés pour le scénario considéré. Comme indiqué précédemment, la plateforme Microsoft offre nativement un ensemble de produits et technologies pour prendre en charge l'identité basée sur les revendications : le service d'émission de jeton de sécurité (STS) fournisseur de revendications prêt à l'emploi pour les entreprises, le Framework pour créer des applications et des services de revendications (authentification, contrôle d'accès, audit, etc.), etc. Dans des environnements hétérogènes réels, ces composants se doivent d'être totalement interopérables.

Pour illustrer cette interopérabilité, MTC Paris Security and Identity Management Interop Lab offre une plateforme dédiée permanente qui propose des scénarios de gestion d'identités multiples, notamment celui décrit dans ce document : c'est-à-dire le scénario de collaboration fédérée utilisant les protocoles OASIS WS-Trust et WS-Federation, Microsoft AD FS 2.0 pour les solutions d'identité et les solutions Microsoft Office 365 pour les ressources de collaboration dans le nuage.

[19] Microsoft Technology Centers : http://microsoft.com/mtc

2 Présentation d'Active Directory Federation Services (AD FS) 2.0

Depuis la plateforme Windows 2000 (Server), l'identité utilisateur Kerberos fournie par AD DS a facilité l'autorisation sécurisée et l'authentification unique sur des ressources Active Directory (Microsoft et non-Microsoft) situées dans des domaines/forêts Active Directory propres ou sécurisées.

AD FS 2.0 permet la fédération des identités, et étend la notion d'authentification centralisée, d'autorisation et d'authentification unique aux applications et services web où qu'ils se trouvent.

Comme précédemment indiqué, la fédération des identités se base sur des protocoles normés pour établir les approbations de fédération entre les fournisseurs de revendications et les parties de confiance, permettant ainsi un accès sécurisé aux applications et services web au-delà des limites de sécurité.

Pour une organisation, AD FS 2.0 fournit aux utilisateurs d'entreprise une expérience fédérée riche et un accès transparent aux ressources situées :

- au sein de l'intranet d'entreprise ;
- en dehors du réseau d'entreprise dans un réseau de périmètre d'entreprise, extranet et/ou sur le nuage, par exemple dans la plateforme Microsoft Windows Azure[20], l'offre PaaS (Microsoft's Platform as a Service) ;
- sur les réseaux de périmètre des organisations partenaires qui rendent disponibles des ressources aux utilisateurs de l'organisation ;
- dans le nuage avec des fournisseurs Saas (Software as a Service) qui prennent en charge l'identité fédérée, par exemple, Microsoft avec ses offres Microsoft Office 365[21] dans le cadre de ce document.

AD FS 2.0 est un composant de la plateforme Windows (Server) et son utilisation est incluse dans le coût de la licence associée.

Remarque importante :

Le rôle AD FS disponible dans Windows Server 2008 (R2) ne correspond pas à AD FS 2.0; il s'agit de la version 1.1 précédente. Le package logiciel AD FS 2.0 pour la version spécifique de votre système d'exploitation (Windows Server 2008 ou Windows Server 2008 R2) est le fichier d'installation AdfsSetup.exe. Pour télécharger ce fichier, accédez à Active Directory Federation Services 2.0 RTW[22].

[20] Plateforme Microsoft Windows Azure : http://www.windowsazure.com/

[21] Microsoft Office 365 : http://office365.microsoft.com/

[22] Active Directory Federation Services 2.0 RTW : http://www.microsoft.com/fr-fr/download/details.aspx?id=10909

Remarque importante :

Au moment de la rédaction de ce document, un correctif cumulatif 2 pour AD FS 2.0 est disponible. Ce correctif cumulatif (ou le précédent[23]) comprend des correctifs et des mises à jour pour AD FS 2.0 RTW très intéressantes dans le cadre de ce document pour la fonctionnalité d'authentification unique d'Office 365. Pour plus d'informations sur ce correctif cumulatif et son téléchargement, voir l'article 2681584 DESCRIPTION DU CORRECTIF CUMULATIF 2 POUR ACTIVE DIRECTORY FEDERATION SERVICES (AD FS) 2.0[24].

2.1 Service d'émission de jeton de sécurité (STS) passif/actif

AD FS 2.0 est un service STS. Ce service peut émettre, valider et échanger des jetons de sécurité.

Les jetons de sécurité se composent de revendications, c'est-à-dire des informations sur les utilisateurs, par exemple nom, id, e-mail, groupe, rôle, privilège ou fonctionnalité, utilisées pour prendre des décisions relatives à l'authentification et à l'autorisation.

Les jetons de sécurité suivent une méthode standard et sécurisée pour créer des packages de revendications pour le transport à partir d'un fournisseur de revendications (partenaire de fédération approuvé qui émet le jeton) vers la partie de confiance (partenaire de fédération de confiance qui comprend et utilise le jeton).

La norme SAML (Security Assertion Markup Language) développée par le comité technique OASIS Security Services (SAML) Technical Committee (TC) (éventuellement en anglais)[25], dont Microsoft Corporation est membre, décrit ce format de jeton de sécurité : le format SAML. Office 365 prend en charge l'assertion/jeton SAML 1.1.

Un service STS peut émettre des jetons dans différents formats et peut protéger le contenu des jetons de sécurité en transit via l'utilisation de certificats X.509 pour la signature du jeton, ce qui permet à une partie de confiance de valider en toute connaissance de cause les fournisseurs de revendications de confiance. (le chiffrement de jeton est également pris en charge.)

Ce concept d'échange comprend le traitement et la transformation du jeton en termes de type d'approbation, format de jeton, sémantiques et (valeurs des) revendications pour l'« adaptation d'impédance ».

Afin de remettre et de traiter les demandes de revendications, AD FS 2.0 comprend un pipeline de revendications, qui représente le chemin que doivent suivre les revendications via le service STS avant de pouvoir être émises dans le cadre du jeton de sécurité. Le service STS gère le processus de bout en bout des revendications pendant les différentes étapes du pipeline, ce qui comprend le traitement des règles de revendication par le moteur de règles de revendication.

Dans ce but, AD FS utilise AD DS comme magasin d'informations d'identification. AD FS 2.0 peut également utiliser des attributs de plusieurs magasins d'attributs, tels que Active Directory Lightweight Directory Services (AD LDS), des bases de données Microsoft SQL Server et d'autres sources de données.

---

[23] Article 2607496 DESCRIPTION DU CORRECTIF CUMULATIF 1 POUR ACTIVE DIRECTORY FEDERATION SERVICES (AD FS) 2.0 : http://support.microsoft.com/kb/2607496

[24] Article 2681584 DESCRIPTION DU CORRECTIF CUMULATIF 2 POUR ACTIVE DIRECTORY FEDERATION SERVICES (AD FS) 2.0 : http://support.microsoft.com/kb/2681584

[25] OASIS Security Services (SAML) Technical Committee (TC) : http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Nous recommandons la lecture de l'article Comprendre les concepts clés avant de déployer AD FS 2.0 (éventuellement en anglais)[26] pour une présentation d'AD FS 2.0.

En conséquence, AD FS 2.0 peut jouer les rôles suivants (et participer à différents types de topologie de schéma d'approbation) :

- **service IP-STS (Identity Provider Security Token Service)** : quand AD FS 2.0 n'a pas configuré de fournisseurs de revendications, à l'exception du magasin d'informations d'identification et de magasins d'attributs facultatifs.

  L'authentification est réalisée par IP-STS par rapport au magasin d'informations d'identification et un jeton de sécurité est émis sur la partie de confiance cible afin que les décisions de contrôle d'accès puissent être prises sur cette base ;

- **service RP-STS (Relying Party STS)** : quand AD FS 2.0 a configuré des fournisseurs de revendications, mais que toutes les méthodes d'authentification locales sont désactivées dans la configuration. AD FS 2.0 indique à l'utilisateur de s'authentifier avec un STS/fournisseur de revendications de confiance.

  Le service RP-STS vérifie le jeton de sécurité présenté par les demandeurs et génère à son tour un jeton de sécurité vers la ressource cible ou la partie de confiance suivante dans la chaîne vers la ressource cible. Dans le dernier cas, il peut émettre un jeton de délégation (Act As tokens) afin de prendre en charge les scénarios de délégation ;

- **Hybride** : quand AD FS 2.0 a configuré des fournisseurs de revendications, et utilise une méthode d'authentification locale activée dans la configuration.

2.2 Fédération dans des environnements hétérogènes

Pour s'adapter à un ensemble de scénarios de fédération ouvert, AD FS 2.0 prend en charge plusieurs normes OASIS largement implémentées et utilisées dans les entreprises : WS-Federation, WS-Trust, SAML 2.0, etc.

De même que dans la version 1.1 précédente, AD FS 2.0 prend en charge le protocole passif WS-Fed (éventuellement en anglais)[27] pour les clients passifs de navigateur. Cette spécification utilise le format d'assertion SAML pour les jetons de sécurité, mais comme son nom l'indique, pas le protocole.

Ce protocole est adopté par la plupart des fournisseurs IDA tiers. C'est pourquoi, la prise en charge par AD FS 2.0 du protocole passif WS-Fed permet potentiellement l'interopérabilité avec les principales solutions du marché. Comme il sera expliqué dans ce document, ce protocole est utilisé pour la fonctionnalité d'authentification unique dans Office 365.

De plus, AD FS 2.0 prend en charge le protocole Security Assertion Markup Language (SAML) 2.0 (éventuellement en anglais)[28] ainsi que les assertions SAML 1.1 et 2.0 (jetons de sécurité). Le livre blanc Utilisation d'AD FS 2.0 pour l'interopérabilité avec l'authentification unique web fédérée SAML 2.0 (éventuellement en anglais)[29] fournit des explications sur les éléments de configuration à prendre en compte lors de l'utilisation d'AD FS 2.0 pour l'interopérabilité avec l'authentification unique web fédérée SAML 2.0.

---

[26] COMPRENDRE LES CONCEPTS CLES AVANT DE DEPLOYER AD FS 2.0 : http://technet.microsoft.com/en-us/library/ee913566(WS.10).aspx

[27] WEB SERVICES FEDERATION LANGUAGE (WS-FEDERATION) VERSION 1.2 : http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf

[28] SECURITY ASSERTION MARKUP LANGUAGE (SAML) 2.0 : http://go.microsoft.com/fwlink/?LinkId=193996

[29] UTILISATION D'AD FS 2.0 POUR L'INTEROPERABILITE AVEC L'AUTHENTIFICATION UNIQUE WEB FEDEREE SAML 2.0 : http://download.microsoft.com/documents/France/Interop/2010/Using_ADFS2_0_For_Interoperable_SAML_2_0-Based_Federated_SSO.docx

Désormais, le protocole SAML (SAML-P) n'est plus pris en charge par la fonctionnalité d'authentification unique d'Office 365.

Remarque :

La spécification SAML définit des assertions, protocoles, liaisons, profils XML, etc. La spécification SAML fait référence à la syntaxe et à la sémantique des assertions SAML ainsi qu'au protocole utilisé pour demander et transporter ces assertions d'une entité système à une autre. Les assertions SAML sont généralement transférées d'un fournisseur de revendications à une partie de confiance. Bien que la fonctionnalité d'authentification unique dans Office 365 ne prenne pas en charge actuellement le protocole SAML 2.0 (SAML-P 2.0), elle utilise pour le jeton d'authentification les assertions SAML 1.1 spécifiées dans la spécification principale SAML 1.1 (éventuellement en anglais)[30].

Remarque :

SAML-P 2.0 sera peut-être ajouté ultérieurement pour la fonctionnalité d'authentification unique dans Office 365 avec une prise en charge limitée.

De plus, AD FS 2.0 offre nativement la possibilité d'une passerelle de protocole en jouant le rôle de passerelle entre les protocoles SAML 2.0 et passif WS-Fed pour la fédération frontale. Le livre blanc GUIDE ETAPE PAR ETAPE : COLLABORATION FEDEREE AVEC SHIBBOLETH 2.0 ET LES TECHNOLOGIES SHAREPOINT 2010[31] décrit cette fonctionnalité dans le cadre de SharePoint 2010.

AD FS 2.0 a passé avec succès les tests d'interopérabilité SAML 2.0 pour ces modes, comme décrit dans le document Procédures de test d'interopérabilité Liberty pour SAML 2.0 version 3.2.2 (éventuellement en anglais)[32] .

Cette fonctionnalité d'AD FS 2.0 est une conséquence d'une annonce majeure (éventuellement en anglais)[33] faite par Microsoft en février 2008 relative aux améliorations apportées au produit en matière d'ouverture, d'interopérabilité et la création de nouvelles opportunités pour les développeurs, les partenaires, les clients et les concurrents.

L'échange d'informations entre les personnes et les organisations, l'interopérabilité entre les applications et les services sont devenues des besoins primordiaux. Microsoft s'est engagé il y a longtemps déjà à améliorer l'interopérabilité, pour répondre aux besoins de ses clients et rendre les produits Microsoft encore plus ouverts et interopérables.

Afin de répondre à ces besoins et enjeux, Microsoft applique quatre principes d'interopérabilité à ses produits les plus utilisés, tels que Windows Server, SharePoint, etc. à partir de maintenant :

---

[30] ASSERTIONS ET PROTOCOLE POUR OASIS SECURITY ASSERTION MARKUP LANGUAGE (SAML) V1.1 : http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf

[31] GUIDE ETAPE PAR ETAPE : COLLABORATION FEDEREE AVEC SHIBBOLETH 2.0 ET LES TECHNOLOGIES SHAREPOINT 2010 : http://download.microsoft.com/documents/France/Interop/2010/Federated_Collaboration_With_Shibboleth_2_0_and_SharePoint_2010_technologies-1_0.docx

[32] PROCEDURES DE TEST D'INTEROPERABILITE LIBERTY POUR SAML 2.0 VERSION 3.2.2 : http://www.projectliberty.org/liberty/content/download/4709/32204/file/Liberty_Interoperability_SAML_Test_Plan_v3.2.2%20.pdf

[33] Communiqué de presse. MICROSOFT MAKES STRATEGIC CHANGES IN TECHNOLOGY AND BUSINESS PRACTICES TO EXPAND INTEROPERABILITY: http://www.microsoft.com/presspass/press/2008/feb08/02-21ExpandInteroperabilityPR.mspx

1. garantir une connexion ouverte à ces produits ;
2. encourager la portabilité des données ;
3. améliorer la prise en charge des normes du domaine ;
4. favoriser l'échange et la collaboration dans l'informatique, notamment avec les communautés Open Source sur l'interopérabilité et les normes.

Ces principes s'appliquent évidemment à AD FS 2.0 dont c'est le but affiché.

En plus des protocoles de navigateur courants, tels que les protocoles passif WS-Fed et SAML 2.0, AD FS 2.0 prend également en charge pour les clients smart la norme OASIS WS-Trust (éventuellement en anglais)[34], qui tire parti de la fonctionnalité d'authentification unique dans Office 365.

Toutes ces fonctionnalités sont reconnues par l'industrie. En effet, à l'occasion de la conférence European Identity Conference (EIC) 2009, l'événement européen majeur pour IAM (Identity and Access Management) et GRC (Governance, Risk Management, and Compliance), la société Kuppinger Cole a attribué la récompense European Identity Award 2009 (éventuellement en anglais)[35], catégorie « Meilleure innovation », à Microsoft pour le projet Geneva (AD FS 2.0 & WIF 1.0), pour lequel la fédération devient une partie intégrante des conteneurs utilisateur, « *l'une des améliorations les plus significatives en matière d'utilisation et de propagation de la fédération des identités* ».

2.3 Terminologie utilisée dans ce livre

Dans le reste de ce document, les termes suivants détaillés dans Tableau 1sont utilisés pour AD FS 2.0.

Tableau 1: Terminologie AD FS 2.0

Terme	Description
Base de données de configuration AD FS 2.0	Une base de données utilisée pour stocker toutes les données de configuration qui représentent une instance AD FS 2.0 ou service de fédération. Ces données de configuration peuvent être stockées à l'aide de la fonctionnalité Base de données interne Windows (WID) fournie avec Windows Server 2008 (R2) ou une base de données Microsoft SQL Server.
Revendication	Une déclaration qu'une entité fait à son propos ou un autre sujet. Par exemple, une déclaration peut être un nom, une adresse de messagerie, un groupe, un privilège ou une fonctionnalité. Les revendications sont émises par des fournisseurs (dans ce contexte, un client Office 365) et une ou plusieurs valeurs leurs sont attribuées. Elles sont également définies par un type de valeur de revendication, et parfois des métadonnées associées.
Service de fédération	Une instance logique d'AD FS 2.0. Un service de fédération peut être déployé sous la forme d'un serveur de fédération autonome (FS) ou d'une batterie de serveurs de fédération d'équilibrage de charge. Le nom du service de fédération prend la valeur par défaut du nom de l'objet du certificat SSL/TLS. Le nom DNS du service de fédération doit être utilisé dans le nom Objet du certificat SSL/TLS.
Serveur de fédération	Un ordinateur exécutant Windows Server 2008 (R2) qui a été configuré pour agir dans le rôle serveur de fédération (FS) pour AD FS 2.0. Un serveur de fédération fait partie d'un service de fédération qui peut émettre, gérer et valider les demandes de jetons de sécurité et de gestion

[34] WS-TRUST VERSION 1.3 : http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf

[35] European Identity Award 2009: http://www.id-conf.com/blog/2009/05/07/awards-for-outstanding-identity-management-projects/

Terme	Description
	des identités. Les jetons de sécurité sont composés d'un ensemble de revendications, par exemple le nom d'un utilisateur ou un rôle.
Batterie de serveurs de fédération	Plusieurs serveurs de fédération dans le même réseau qui sont configurés pour agir comme une instance de service de fédération.
Serveur proxy de fédération	Un ordinateur exécutant Windows Server 2008 (R2) qui a été configuré pour agir en tant que service de proxy intermédiaire entre un client sur Internet et un service de fédération situé derrière un pare-feu sur un réseau d'entreprise. Afin d'autoriser l'accès distant aux services dans Office 365, par exemple à partir d'un smartphone, d'un ordinateur personnel ou d'une borne Internet, vous devez déployer un serveur proxy de fédération (FS-P).
Partie de confiance	Un service de fédération AD FS 2.0, une solution de fédération tierce, une application ou un service qui utilise des revendications dans une transaction donnée.
Approbation de partie de confiance	Dans le composant logiciel enfichable Gestion AD FS 2.0, une approbation de partie de confiance est un objet d'approbation qui est créé pour maintenir la relation avec un autre service de fédération, application ou service (dans le cas d'Office 365) qui utilise des revendications du service de fédération de votre organisation.
Équilibrage de charge réseau	Une application dédiée (par exemple, équilibrage de la charge réseau) ou un matériel (par exemple un commutateur multicouche) utilisé pour fournir la tolérance de panne, la haute disponibilité et l'équilibrage de charge entre plusieurs nœuds. Pour AD FS 2.0, le nom DNS de cluster que vous créez à l'aide de ce NLB doit correspondre au nom du service de fédération que vous avez spécifié quand vous avez déployé votre premier serveur de fédération dans votre batterie de serveurs.

Remarque :

Pour plus d'informations sur AD FS 2.0 en plus du contenu de ce livre, consultez la documentation du produit (éventuellement en anglais)[36], et le forum aux questions AD FS 2.0 (éventuellement en anglais)[37] dédié.

2.4 Remarques sur les types de déploiement

2.4.1 Prérequis et configuration logicielle

Afin d'installer un serveur de fédération, Microsoft Active Directory Federation Services (AD FS) 2.0 Release to Web (RTW)[38][39] nécessite Windows Server 2008 Service Pack 2 (SP2) ou Windows Server 2008 R2 en termes de système d'exploitation serveur Windows.

[36] Documentation TechNet AD FS 2.0 : http://technet.microsoft.com/en-us/library/adfs2(WS.10).aspx

[37] Forum aux questions AD FS 2.0 : http://social.msdn.microsoft.com/Forums/en-US/Geneva/threads

[38] Téléchargement Microsoft AD FS 2.0 Release to Web (RTW) : http://www.microsoft.com/downloads/details.aspx?FamilyID=118c3588-9070-426a-b655-6cec0a92c10b

[39] Téléchargement Microsoft AD FS 2.0 : http://www.microsoft.com/downloads/details.aspx?FamilyID=118c3588-9070-426a-b655-6cec0a92c10b

> **Remarque :**
>
> *Comme déjà indiqué, un rôle serveur est déjà installé sur Windows Server 2008 et Windows Server 2008 R2 pour AD FS. Il ne s'agit pas de la version correcte (version 1.1), la version 2.0 est requise pour la fonctionnalité d'authentification unique d'Office 365.*

Les prérequis logiciels suivants sont nécessaires pour AD FS 2.0 RTW :

- Internet Information Services (IIS) 7 ou 7.5 en fonction de la version Windows Server ;
- Microsoft .NET Framework 3.5 SP1.

Pour plus d'informations sur la configuration système requise, consultez la page d'accueil AD FS 2.0 (éventuellement en anglais)[40].

Vous devez installer les correctifs AD FS 2.0 après avoir installé AD FS 2.0. Comme mentionné précédemment, un correctif cumulatif 2 pour AD FS 2.0 est disponible. Ce correctif cumulatif comprend des correctifs et des mises à jour pour AD FS 2.0 RTW très intéressants dans le cadre de ce document pour la fonctionnalité d'authentification unique d'Office 365.

2.4.2 Service de fédération

Comme suggéré par la terminologie ci-dessus, il existe deux types de déploiement pour les serveurs de fédération AD FS 2.0 : autonome et batterie de serveurs.

Un serveur de fédération autonome est une instance unique du service de fédération. Vous créez un serveur de fédération autonome quand votre environnement de production est de petite taille ou si vous êtes en période d'évaluation de la technologie AD FS 2.0.

Une batterie de serveurs de fédération (à charge équilibrée) contient plusieurs serveurs de fédération, qui hébergent la même instance d'un service de fédération. Inversement, vous créez une batterie quand vous avez besoin d'une haute disponibilité et de l'équilibrage de charge. La création d'un nouveau service de fédération pour un scénario de batterie de serveurs fera du premier ordinateur de la batterie de serveur le serveur de fédération principal pour la batterie de serveurs.

2.4.3 Stockage des informations de configuration

Dans AD FS 2.0, les informations de configuration sont stockées dans une base de données. Un serveur de fédération autonome stocke ses informations de configuration localement dans la base de données interne Windows (WID).

WID n'a pas besoin d'être installé manuellement, elle est installée par la première application ou le premier service qui en a besoin. WID exécute son propre service Windows et est incluse avec Windows Server 2008 et Windows Server 2008 R2. WID est une variante de SQL Server Express et est conçue pour les applications ou services en boîte qui ont besoin d'un serveur backend SQL.

La base de données WID est en lecture/écriture dans un serveur de fédération autonome, tandis que dans des scénarios de batterie de serveurs de fédération (à charge équilibrée), la base de données est en lecture/écriture sur le serveur de fédération principal et en lecture seule sur les serveurs de fédération secondaires de la batterie. Les serveurs de fédération secondaires se connectent et synchronisent les données avec le serveur de fédération principal dans la batterie en l'interrogeant à intervalles réguliers pour voir si les données ont changé. Les serveurs de fédération secondaires existent pour fournir la tolérance de panne pour le serveur de fédération principal tout en équilibrant la charge pour les demandes d'accès.

---

[40] Page d'accueil AD FS 2.0 : http://www.microsoft.com/adfs2

Les informations de configuration peuvent être également stockées dans une base de données SQL Server, ce qui permet des fonctionnalités supplémentaires, telles que des améliorations des performances (notamment la possibilité de montée en charge en utilisant plus de 5 serveurs de fédération, ce qui est la limite pour la base de données WID par batterie), la détection de relecture de jeton SAML et la résolution d'artefact SAML. Pour plus d'informations, consultez l'article Batterie de serveurs de fédération avec SQL Server (éventuellement en anglais)[41].

2.4.4 Proxys

2.4.4.1 Serveur proxy de fédération AD FS 2.0

Le rôle serveur proxy de fédération peut être déployé sur le réseau de périmètre pour améliorer la sécurité et les performances de l'installation AD FS 2.0 en fournissant les avantages suivants :

- **Sécurité :** le serveur proxy de fédération fournit une couche supplémentaire de défense en isolant les demandes frontales des demandes principales correspondantes au service de fédération protégé, qu'il s'agisse d'un serveur de fédération autonome ou d'une batterie de serveurs de fédération (à charge équilibrée). Le serveur proxy de fédération traite uniquement les demandes envoyées à des préfixes HTTP connus. Il peut également fournir une valeur supplémentaire en validant les données dans les requêtes (par exemple, en validant les certificats) au nom d'AD FS 2.0 ;
- **Protection de clé** : la clé de signature de jetons privée et la clé d'identité de service pour AD FS 2.0 ne sont pas stockées sur le serveur proxy de fédération ;
- **Ressources d'entreprises** : le serveur proxy de fédération peut traiter les demandes client AD FS 2.0 sans demander l'accès aux ressources d'entreprise, telles que Active Directory ;
- **Mise en cache** le serveur proxy de fédération peut potentiellement décharger le serveur de fédération en mettant en cache le contenu HTTP statique.

Un autre avantage de l'utilisation d'un serveur proxy de fédération est que vos utilisateurs externes qui ne sont pas joints au domaine pourront voir une page d'authentification basée sur les formulaires plutôt que l'invite d'authentification standard.

Tout comme le rôle de serveur de fédération, le rôle de serveur proxy de fédération peut être déployé en tant que serveur proxy de fédération autonome ou batterie de serveurs serveur proxy de fédération (à charge équilibrée).

2.4.4.2 Autres proxys

Un proxy tel que Microsoft Threat Management Gateway (TMG) qui peut exposer/publier les points de terminaison de service de fédération AD FS 2.0 (voir section n°5.1.5 POINTS DE TERMINAISON) du réseau de périmètre sur Internet. Pour plus d'informations, consultez le billet de blog Publication ADFS via ISA ou TMG Server (éventuellement en anglais)[42].

(Il est également possible d'implémenter AD FS 2.0 à partir d'un appareil Microsoft Forefront Unified Application Gateway (UAG) Service Pack 1 (SP1). Une description de la configuration d'UAG SP1 pour AD FS 2.0 est fournie dans l'article Déploiement de la fédération avec AD FS (éventuellement en anglais)[43] de la documentation UAG.)

---

[41] BATTERIE DE SERVEURS DE FEDERATION AVEC SQL SERVER : http://technet.microsoft.com/en-us/library/gg982487(WS.10).aspx

[42] PUBLICATION ADFS VIA ISA OU TMG SERVER: http://blog.c7solutions.com/2011/06/publishing-adfs-through-isa-or-tmg.html

[43] DEPLOIEMENT DE LA FEDERATION AVEC AD FS : http://technet.microsoft.com/en-us/library/dd857388.aspx

3 Authentification fédérée dans Microsoft Office 365

L'option de configurer AD FS 2.0 revient à chaque société individuelle et il est important de connaître le comportement attendu et l'expérience obtenue. À l'exception des sites Internet pour les accès anonymes créés avec SharePoint Online, les utilisateurs doivent être authentifiés pour accéder aux services dans Office 365.

Dans ce but, Microsoft Office 365 propose deux types d'identités :

1. **ID sur le nuage Microsoft Online Services (identité sur le nuage)** : les utilisateurs reçoivent, pour se connecter aux services dans Office 365, des informations d'identification nuage séparées des autres informations d'identification locales d'entreprise ou de bureau. Les identités sur le nuage sont masterisées dans le service/nuage.

> **Remarque :**
>
> *Avec la synchronisation d'annuaires facultative, les identifiants utilisateur masterisés localement peuvent être synchronisés avec le service/nuage sous la forme d'identités sur le nuage.*

2. **ID fédérées (identité fédérée)** : dans les sociétés avec un Active Directory local, la fonctionnalité d'authentification unique peut être utilisée. Les utilisateurs peuvent se connecter aux services dans Office 365 à l'aide de leurs informations d'identification d'entreprise Active Directory. Les ID des utilisateurs sont masterisés localement dans Active Directory et synchronisés avec le service sous la forme d'identités fédérées.

Les utilisateurs accèdent à Office 365 en s'authentifiant sur leurs comptes utilisateur Office 365, via une invite réclamant des informations d'identification valides ou via un processus d'authentification unique. Une fois authentifié, les identités des utilisateurs font référence aux noms d'utilisateur associés aux comptes Office 365. C'est pourquoi, trois types d'authentification sont disponibles :

1. identités sur le nuage ;
2. identités sur le nuage + synchronisation d'annuaires (DirSync) ;
3. identités fédérées + synchronisation d'annuaires (DirSync).

Le type d'identité (nuage ou fédéré) affecte l'expérience utilisateur, les exigences d'administration, les éléments de déploiement et les fonctionnalités utilisant Office 365.

Vous trouverez ci-dessous une explication des différents cas :

- **Expérience utilisateur avec des identités sur le nuage** : les utilisateurs se connectent avec leur identité sur le nuage. Les identités sur le nuage sont authentifiées à l'aide d'une stimulation/réponse traditionnelle, c'est-à-dire que les utilisateurs tapent leur nom d'utilisateur et leur mot de passe. L'authentification se produit sur le nuage. Les utilisateurs sont toujours invités à fournir des informations d'identification.

  Comment indiqué ci-dessus, les utilisateurs ont deux identifiants, un pour accéder aux services locaux et un pour les services dans Office 365 (l'ID de nuage Microsoft Online Services). Il en résulte que les utilisateurs sont invités à fournir leurs informations d'identification, même quand ils sont connectés à leur domaine AD, quand ils veulent accéder aux services Office 365. Il est possible de sélectionner l'option de sauvegarde du mot de passe dans de nombreux cas pour simplifier le processus.

- **Expérience utilisateur avec des identités fédérées** : les utilisateurs se connectent avec leur ID d'entreprise pour accéder aux services en ligne et d'entreprise. En d'autres termes, ils sont

authentifiés de façon transparente à l'aide d'AD FS 2.0 lors de l'accès aux services Office 365. L'authentification se produit localement par rapport à l'annuaire Active Directory de l'organisation et les utilisateurs bénéficient réellement de l'authentification unique. De plus, l'authentification à 2 facteurs (2 Factor Authentication, 2FA) peut être utilisée si elle est déployée localement.

- **Expérience administrateur avec des identités sur le nuage** : les administrateurs de l'organisation gèrent la stratégie de mot de passe localement et sur le nuage. La stratégie de mot de passe pour les identités sur le nuage est stockée dans le nuage avec le service Office 365. La réinitialisation de mot de passe doit être gérée pour les ID sur le nuage Microsoft Online Services et les ID locaux et les utilisateurs doivent donc changer leur mot de passe pour les deux selon la stratégie. Enfin, il n'y a pas d'intégration 2FA.
- **Expérience administrateur avec des identités fédérées** : les administrateurs de l'organisation gèrent la stratégie de mot de passe locale uniquement et donc ne se préoccupent pas de la réinitialisation des mots de passe pour les identités fédérées. L'annuaire Active Directory de l'organisation stocke et contrôle la stratégie de mot de passe. La réinitialisation de mot de passe se produit uniquement pour les identifiants locaux. Plusieurs options d'intégration 2FA sont proposées (voir section n° 6.2 PRISE EN CHARGE DE L'AUTHENTIFICATION FORTE (2FA) POUR OFFICE 365).

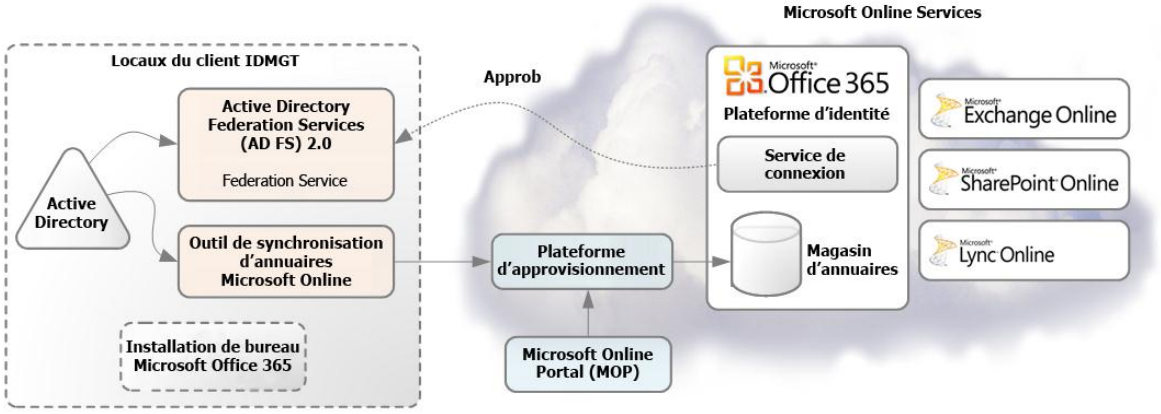


Figure 1Plateforme d'identité Office 365

Le reste de ce document traite de la fonctionnalité d'authentification unique et des identités fédérées dans ce contexte. Pour des informations spécifiques sur les identités sur le nuage Office 365, telles que la création de compte utilisateur, la stratégie de mot de passe, etc., consultez le livre intitulé Description du service d'identité Office 365 (éventuellement en anglais)[44] comme point de départ.

3.1 Éléments requis pour les identités fédérées

3.1.1 Éléments requis pour Active Directory

Afin qu'une organisation puisse tirer parti de la fonctionnalité d'authentification unique d'Office 365, les contrôleurs de domaine doivent exécuter au moins Windows Server 2003 ou une version ultérieure avec un niveau fonctionnel mode mixte ou natif.

[44] DESCRIPTION DU SERVICE D'IDENTITE OFFICE 365 : http://www.microsoft.com/download/en/details.aspx?id=13602

3.1.2 Éléments requis pour les ordinateurs de travail

Les Service Packs de Windows XP, Windows Vista ou Windows 7 les plus récents doivent être installés sur les ordinateurs de travail. De plus, pour assurer la découverte et l'authentification des services dans Office 365, un ensemble de composants et de mises à jour doivent être appliqués à chaque ordinateur qui utilise des clients riches (par exemple, Office Professionnel Plus 2010) et qui se connecte à Office 365.

Plutôt que d'installer manuellement les mises à jour, une par une, Microsoft fournit un package d'installation automatisé (application Configuration du bureau Office 365), qui configure automatiquement les stations de travail avec les mises à jour requises. Cette application remplace le Connecteur Microsoft Online Services. Si l'application Configuration du bureau Office 365 est installée sur les ordinateurs de travail, tous les éléments requis pour le système d'exploitation sont déjà installés.

L'application Configuration du bureau Office 365 fournit plusieurs avantages, notamment :

- la détection automatique des mises à jour nécessaires ;
- l'installation des mises à jour et des composants après approbation ou sans assistance à partir de la ligne de commande ;
- la configuration automatique d'Internet Explorer et de Lync pour une utilisation avec Office 365.

> **Remarque :**
>
> *Une liste des mises à jour requises est publiée pour les organisations qui souhaitent utiliser une autre méthode de déploiement des mises à jour. L'article Installer manuellement les mises à jour de bureau Office 365 (éventuellement en anglais)[45] décrit la liste des mises à jour requises.*

L'application Configuration du bureau Office 365 est disponible au téléchargement à partir de Microsoft Online Portal (MOP). Pour les clients web, tels que SharePoint Online, Outlook Web App (OWA), etc. il n'est pas nécessaire d'installer l'application Configuration du bureau Office 365, elle n'est nécessaire que pour les clients tels que Outlook et Lync.

L'une des fonctionnalités clés de l'application Configuration du bureau Office 365 est l'Assistant de connexion Microsoft Online Services (MOS SIA). Ce n'est pas la seule fonctionnalité de l'application Configuration du bureau Office 365, mais elle est importante dans le cadre de ce document.

> **Remarque :**
>
> *Le téléchargement Assistant de connexion Microsoft Online Services pour les professionnels des technologies de l'information RTW[46] (msoidcli_32bit.msi pour les systèmes 32 bits ou msoidcli_64bit.msi pour les systèmes 64 bits) est conçu pour les informaticiens, pour une distribution sur les systèmes client gérés dans le cadre d'un déploiement client Office 365, via System Center Configuration Manager (SCCM) ou des systèmes de distribution de logiciels similaires. Pour les utilisateurs qui installent Office 365 via l'application Configuration du bureau Office 365, ce téléchargement n'est pas nécessaire, car MOS SIA est installé avec la Configuration du bureau comme indiqué ci-dessus.*

[45] INSTALLER MANUELLEMENT LES MISES A JOUR DE BUREAU OFFICE 365 : http://community.office365.com/en-us/w/administration/manually-install-office-365-desktop-updates.aspx

[46] Assistant de connexion Microsoft Online Services pour les professionnels des technologies de l'information RTW : http://www.microsoft.com/fr-fr/download/details.aspx?id=28177

Comme décrit dans l'article de la communauté Description de l'Assistant de connexion Microsoft Online Services (MOS SIA) (éventuellement en anglais)[47], les composants de MOS SIA se composent d'un ensemble de DLL et d'un service Windows. Ces composants sont appelés par les applications de bureau, telles que Abonnement Office et Lync pour authentifier les utilisateurs sur Office 365, et donc pour exécuter la demande de jeton d'authentification. Cela se produit via AD FS 2.0 en arrière-plan.

La relation d'architecture entre les composants indiquée ci-dessous.

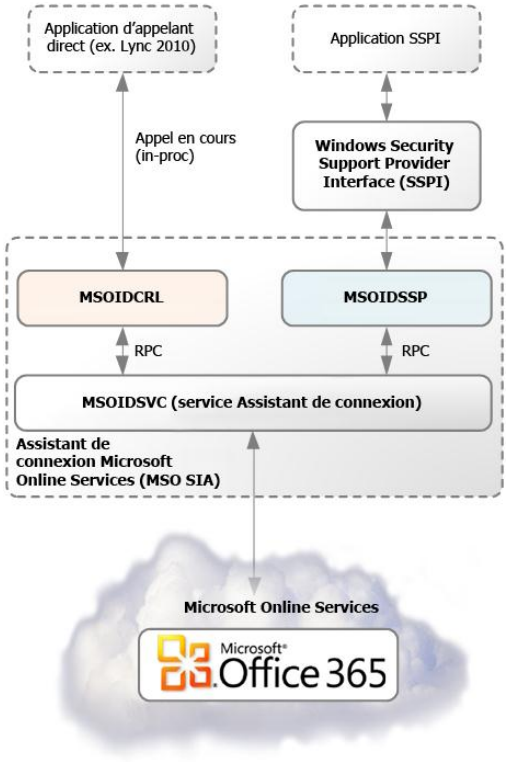


Figure 2Vue d'ensemble de l'architecture de l'Assistant de connexion Microsoft Online Services

[47] DESCRIPTION DE L'ASSISTANT DE CONNEXION MICROSOFT ONLINE SERVICES (MOS SIA) : http://community.office365.com/en-us/w/office/534.aspx

Remarque :

L'interface SSPI Windows (Security Support Provider Interface) est une interface logicielle avec une API commune clairement définie permettant l'obtention des services de sécurité intégrée pour l'authentification (ainsi que l'intégrité des messages, la confidentialité des messages et la qualité de service de sécurité) pour n'importe quel protocole d'application distribuée. Un ou plusieurs modules logiciels fournissent les fonctionnalités d'authentification. Chaque module, appelé fournisseur SSP, est implémenté sous la forme d'une DLL. Un fournisseur SSP fournit un ou plusieurs packages de sécurité. Divers fournisseurs SSP et packages sont disponibles. Windows comprend le package de sécurité NTLM et le package de sécurité de protocole Microsoft Kerberos. De plus, vous pouvez installer le package de sécurité SSL (Secure Socket Layer) ou l'un des fournisseurs SSP compatibles SSPI.

Pour plus d'informations sur SSPI, consultez l'article Microsoft TechNet Interface SSP (Security Support Provider) (éventuellement en anglais)[48] et l'article Microsoft MSDN Interface SSPI (Security Support Provider Interface) (éventuellement en anglais)[49].

Les fichiers binaires suivants sont installés dans le dossier *%Program Files%\Common Files\Microsoft Shared\Microsoft Online Services*.

- *MSOIDCLI.dll* : fichier qui peut être chargé directement par les applications qui doivent authentifier des utilisateurs sur Office 365 ;
- *MSOIDSVC.exe* : installé en tant que service Windows avec le nom MSOIDSVC. Il s'agit d'un composant central qui exécute les demandes de connexion et de ticket de service sur le service de fédération AD FS 2.0 local et le service de connexion de la plateforme des identités Office 365 ;
- *MSOIDSVCM.exe* : processus de surveillance qui surveille le service MSOIDSVC. Il est lancé quand le service MSOIDSVC démarre ;
- *MSOIDRES.dll* : fichier de ressources qui contient les chaînes de texte localisées pour les messages d'erreur.

Les DLL supplémentaires suivantes sont installées sur les systèmes Windows 7 :

- *MSOIDCredProv.dll* : composant Fournisseur d'informations d'identification Windows enregistré en tant qu'objet COM dans le système ;
- *MSOIDSSP.dll* : composant SSP installé dans le dossier *%windir%\system32*.

Remarque :

Sur les versions 64 bits de Windows, msoidcli.dll et msoidres.dll sont installés dans le dossier %Program Files (x86)%\Common Files\Microsoft Shared\Microsoft Online Services. Sur les versions 64 bits de Windows 7, msoidcredprov.dll est également installé dans ce dossier.

Les clés et valeurs de registre suivantes sont créées ou mises à jour pendant l'installation de MOS SIA.

[48] INTERFACE SSP (SECURITY SUPPORT PROVIDER) : http://technet.microsoft.com/en-us/library/bb742535.aspx

[49] INTERFACE SSPI (SECURITY SUPPORT PROVIDER INTERFACE) : http://msdn.microsoft.com/fr-fr/library/windows/desktop/aa378663(v=vs.85).aspx

> **Remarque :**
>
> *Les données de certaines valeurs dépendent de la version et de la langue utilisées.*

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSOIdentityCRL]
"Language" (default: dword:00000409)
"TargetDir" (default: %Program Files%\Common Files\Microsoft Shared\Microsoft Online Services)
"MSOIDCRLVersion" (as of writing, current version is 7.250.4287.0)

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSOIdentityCRL\Environment]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSOIdentityCRL\Environment\Production]
"RemoteFile" (default: http://clientconfig.microsoftonline-p.net/PPCRLconfig.srf)


"Flags" (default: dword:00000001)
"Level" (default: dword:00000002)
```

Bien que MOS SIA soit fourni avec le bureau Office 365, la Configuration du bureau Office 365 n'est pas un service d'authentification ou de connexion, et ne doit pas être confondu avec l'authentification unique. Pour plus d'informations sur la Configuration du bureau Office 365, voir la rubrique d'aide en ligne Office 365 CONFIGURER MON BUREAU POUR OFFICE 365[50].

3.1.3 Éléments requis pour le serveur de fédération AD FS 2.0

Il est à noter que l'application Configuration du bureau Office 365 doit être installée sur tous les ordinateurs qui se connecteront à Office 365, y compris les ordinateurs du service de fédération AD FS 2.0. Cela est requis sur les serveurs de fédération par l'outil Module Microsoft Online Services pour Windows PowerShell, afin qu'une connexion à l'environnement Office 365 puisse être établie avec Windows PowerShell pour fédérer le domaine.

> **Remarque :**
>
> *Windows PowerShell est un interpréteur de commandes et un langage de script conçu pour l'administration système et l'Automation. Il utilise des tâches d'administration appelées applets de commande (cmdlet). Chaque applet de commande utilise des arguments requis et facultatifs, appelés paramètres, qui identifient les objets sur lesquels agir et contrôlent la façon dont l'applet exécute sa tâche. Vous pouvez combiner des applets de commande dans des scripts pour exécuter des fonctions complexes qui vous donnent davantage de contrôle et vous aident à automatiser l'administration de Windows et des applications. Les applets de commande sont fréquemment utilisées pour gérer la dernière génération des produits Microsoft Server localement et sur le nuage.*
>
> *Pour plus d'informations sur Windows PowerShell 2.0, voir le site web Windows PowerShell[51], l'aide en ligne Windows PowerShell[52], et le blog web Windows PowerShell (éventuellement en anglais)[53] Windows PowerShell Software Development Kit (SDK) (éventuellement en anglais)[54] qui comprend un guide du programmeur avec des références complètes.*

---

[50] CONFIGURER MON BUREAU POUR OFFICE 365 : http://onlinehelp.microsoft.com/fr-fr/Office365-enterprises/ff637594.aspx

[51] Site web Windows PowerShell : http://www.microsoft.com/powershell

[52] Aide en ligne Windows PowerShell : http://technet.microsoft.com/fr-fr/library/bb978526.aspx

[53] Blog web Windows PowerShell : http://blogs.msdn.com/powershell

[54] SDK Windows PowerShell : http://msdn2.microsoft.com/en-us/library/aa830112.aspx

Le Module Microsoft Online Services est dépendant de l'Assistant de connexion Microsoft Online Services (MSO SIA) fourni avec l'application Configuration du bureau Office 365.

Pour installer l'application Configuration du bureau Office 365 sur le serveur de fédération AD FS 2.0, l'opération est identique à l'installation client.

3.2 Expérience de connexion pour les identités fédérées

L'expérience de connexion change en fonction du type d'identité Office 365 utilisé. L'expérience de connexion de l'utilisateur final dépend des types de client, des méthodes d'accès (au sein ou en dehors du réseau d'entreprise) et si l'ordinateur est joint ou n'est pas joint au domaine.

tableau 2présente les combinaisons clés pour un ordinateur joint au domaine et décrit l'expérience qui en résulte.

Le tableau 2: Expérience de connexion d'identité fédérée avec Office 365 avec un ordinateur joint au domaine

Application	Au sein du réseau d'entreprise	En dehors du réseau d'entreprise
Outlook 2010/Outlook 2007, Exchange ActiveSync, POP, IMAP	demande des informations d'identification lors de la première connexion (et à chaque changement de mot de passe) avec une case à cocher pour les enregistrer.	
Microsoft Online Portal, SharePoint Online, Office Web Apps	boîte de dialogue contextuelle permettant de se connecter en un clic sans entrer les informations d'identification[1]	boîte de dialogue contextuelle permettant de se connecter en un clic et demande des informations d'identification[1]
Outlook Web Apps	connexion transparente sans demande	demande des informations d'identification
applications Office 2010/Office 2007 avec SharePoint Online	boîte de dialogue contextuelle permettant de se connecter en un clic sans entrer les informations d'identification	
Lync 2010 avec Lync Online	connexion transparente sans demande	

[1] Toutes les applications nécessitent que vous tapiez votre nom d'utilisateur ou cliquiez pour vous connecter. Cela peut être changé en utilisant des liaisons intelligentes (voir section n°6.4 UTILISATION DE LIAISONS INTELLIGENTES POUR OFFICE 365).

Comme indiqué dans le tableau ci-dessus, lors de l'utilisation d'identités fédérées, les utilisateurs finaux n'auront pas besoin de fournir leurs mots de passe sur des ordinateurs joints au domaine dans de nombreux cas :

- lors de l'accès à Microsoft Online Portal (MOP), SharePoint Online ou Outlook Web Apps (OWA) via un navigateur, au sein du réseau d'entreprise ;
- lors de l'utilisation d'applications Office 2007 ou 2010 pour accéder aux ressources SharePoint Online ;
- lors de l 'utilisation de Lync 2010 pour accéder à Lync Online.

Les utilisateurs Outlook devront fournir leurs informations d'identification la première fois qu'ils se connectent, et pourront à cette occasion choisir d'enregistrer leur mot de passe. Dans ce cas, les utilisateurs finaux n'auront plus à fournir leur mot de passe, jusqu'au prochain changement qui dépend des stratégies de mot de passe de l'organisation.

tableau 3présente les combinaisons clés pour un ordinateur qui n'est pas joint au domaine et décrit l'expérience qui en résulte.

Le tableau 3: Expérience de connexion d'identité fédérée avec Office 365 sans un ordinateur joint au domaine

Application	Au sein du réseau d'entreprise	En dehors du réseau d'entreprise
Outlook 2010/Outlook 2007, Exchange ActiveSync, POP, IMAP	demande des informations d'identification lors de la première connexion (et à chaque changement de mot de passe) avec une case à cocher pour les enregistrer.	
Microsoft Online Portal, SharePoint Online, Office Web Apps	boîte de dialogue contextuelle permettant de se connecter en un clic et demande des informations d'identification[1]	
Outlook Web Apps	demande des informations d'identification	
applications Office 2010/Office 2007 avec SharePoint Online	boîte de dialogue contextuelle permettant de se connecter en un clic et demande des informations d'identification	
Lync 2010 avec Lync Online	demande des informations d'identification	

[1] Toutes les applications nécessitent que vous tapiez votre nom d'utilisateur ou cliquiez pour vous connecter. Cela peut être changé en utilisant des liaisons intelligentes (voir section n°6.4 UTILISATION DE LIAISONS INTELLIGENTES POUR OFFICE 365).

3.3 Types d'authentification pour les identités fédérées

Cette section traite des types d'authentification utilisateur qui fonctionnent avec Office 365 pour une identité fédérée.

3.3.1 Authentification à partir d'un navigateur web

Comme indiqué précédemment, Office 365 propose plusieurs services accessibles à partir d'un navigateur web, notamment Microsoft Online Portal (MOP), SharePoint Online, et Outlook Web App (OWA). Quand vous accédez à ces services, votre navigateur est redirigé vers une page de connexion sur laquelle vous fournissez vos informations d'identification.

L'expérience de connexion est la suivante pour une identité fédérée :

1. Le navigateur web est redirigé vers le service de connexion Office 365, sur lequel vous tapez votre identifiant d'entreprise au format nom d'utilisateur principal (UPN) (éventuellement en anglais)[55] selon la norme IETF RFC 822 Standard for ARPA Internet Text Messages (éventuellement en anglais)[56], par exemple, xyz@idmgt.com. Le service de connexion détermine que vous faites partie d'un domaine fédéré et propose de vous rediriger sur le service AD FS 2.0 local pour authentification.
2. Si vous avez ouvert une session sur l'ordinateur (joint au domaine), vous êtes authentifié à l'aide de l'authentification Windows intégrée (Kerberos ou NTLMv2) et AD FS 2.0 génère un jeton de connexion SAML 1.1, que le navigateur web publie sur le service de connexion Office 365. À l'aide de ce jeton de connexion, le service de connexion génère un jeton d'authentification que le navigateur web publie sur le service demandé et vous connecte.

Si vos ordinateurs utilisent Extended Authentication Protection (EAP)[57], et que vous utilisez Firefox, Chrome, ou Safari, il se peut que vous ne puissiez pas vous connecter à Office 365 à l'aide de

[55] Attribut UPN (nom d'utilisateur principal) : http://msdn.microsoft.com/en-us/library/windows/desktop/ms680857(v=vs.85).aspx

[56] RFC 822 STANDARD FOR ARPA INTERNET TEXT MESSAGES : http://tools.ietf.org/html/rfc822

[57] Protection étendue pour l'authentification : http://support.microsoft.com/kb/968389/fr-fr

l'authentification Windows intégrée (IWA) au sein d'un réseau d'entreprise. Si ce problème se pose, les utilisateurs peuvent recevoir des invites de connexion régulièrement comme décrit dans l'article Vous recevez des invites à répétition pour entrer vos informations d'identification lorsque vous essayez de vous connecter au point de terminaison du service AD FS 2.0 dans Office 365[58]. Cela est dû à la configuration par défaut (sur Windows 7 et les systèmes d'exploitation clients avec correctifs) pour AD FS 2.0 et EAP.

Jusqu'à ce que Firefox, Chrome, et Safari prennent en charge la fonctionnalité EAP, l'option recommandée pour les clients qui veulent accéder aux services dans Office 365 consiste à installer et à utiliser Windows Internet Explorer 8 et version ultérieure. Si vous voulez utiliser l'authentification unique pour Office 365 avec Firefox, Chrome, ou Safari, vous pouvez essayer les approches suivantes qui peuvent entraîner des problèmes de sécurité :

- désinstaller les correctifs de la protection étendue de l'authentification des ordinateurs ;
- modifier le paramètre de la protection étendue de l'authentification sur le serveur AD FS 2.0 via l'applet de commande **Set-ADFSProperties** :

```
PS C:\Windows\system32> Add-PSSnapin Microsoft.Adfs.Powershell
PS C:\Windows\system32> Set-ADFSProperties –ExtendedProtectionTokenCheck:None
```

> **Remarque :**
>
> *Pour plus d'informations, voir la section Administration AD FS 2.0 avec Windows PowerShell (éventuellement en anglais)[59] du GUIDE DE FONCTIONNEMENT AD FS 2.0 et le guide de référence des applets de commande AD FS 2.0 (éventuellement en anglais) [60].*

- reconfigurer les paramètres d'authentification pour la page AD FS 2.0 sur chaque serveur de fédération à partir de l'authentification Windows intégrée (IWA) pour utiliser l'authentification basée sur les formulaires (FBA) comme décrit dans l'article Vue d'ensemble du gestionnaire d'authentification (éventuellement en anglais)[61].

3.3.2 Authentification à partir d'applications clientes riches

Les clients riches comprennent les applications de bureau Microsoft Office installées sur un ordinateur. L'authentification à partir de ces types d'applications peut s'effectuer de deux manières :

1. **Assistant de connexion Microsoft Online Services (MOS SIA)** : l'Assistant de connexion Microsoft Online Services (installé par l'application Configuration de bureau Office 365) contient le service Windows *MSOIDSVC.exe* qui obtient un jeton d'authentification à partir du service de connexion Office 365 et le renvoie au client riche.

   Avec une identité fédérée, comme décrit plus bas dans ce document (voir section n° 5.3 Présentation du flux d'authentification profil MEX/client riche), le service MSOIDSVC contacte tout d'abord le service de fédération AD FS 2.0 pour authentifier les informations d'identification (à l'aide de Kerberos ou NTLMv2) et obtient un jeton de connexion qui est

[58] Vous recevez des invites à répétition pour entrer vos informations d'identification lorsque vous essayez de vous connecter au point de terminaison du service AD FS 2.0 dans Office 365 : http://support.microsoft.com/kb/2461628/fr-fr

[59] ADMINISTRATION AD FS 2.0 AVEC WINDOWS POWERSHELL : http://go.microsoft.com/fwlink/?LinkId=194005&clcid=0x40C

[60] Guide de référence des applets de commande AD FS 2.0 : http://go.microsoft.com/fwlink/?LinkId=177389&clcid=0x40C).

[61] VUE D'ENSEMBLE DU GESTIONNAIRE D'AUTHENTIFICATION : http://msdn.microsoft.com/fr-fr/library/ee895365.aspx

envoyé au service de connexion Office 365 (à l'aide des informations de métadonnées (WS-Federation) et WS-Trust).

2. **Authentification de base/proxy sur SSL** : le client Outlook passe les informations d'identification de base via SSL à Exchange Online. Exchange Online transfère par proxy la demande d'authentification vers le service de connexion Office 365, puis vers AD FS 2.0 localement (pour l'authentification unique). Le flux d'authentification est décrit plus loin dans ce document (voir section n°5.4 Présentation du flux d'authentification profil authentification de base/active EAS).

> **Remarque importante :**
>
> *Cette authentification nécessite le déploiement d'un serveur proxy ou d'un serveur proxy de fédération AD FS 2.0 sur votre réseau de périmètre (également connu sous le nom de zone démilitarisée, DMZ, ou sous-réseau filtré).*

tableau 4décrit en détail les mécanismes d'authentification avec une identité fédérée pour les différentes combinaisons applications/systèmes d'exploitation.

Le tableau 4: Mécanismes d'authentification pour une identité fédérée dans Office 365

Application	Mécanisme d'authentification
Outlook 2007/Outlook 2010, Exchange ActiveSync, client POP/IMAP/SMTP	authentification de base sur SSL, authentifié via le serveur proxy de fédération AD FS 2.0 (scénario AD FS 2.0 totalement implémenté)
Navigateur web	connexion web, WS-Federation (AD FS 2.0)
Microsoft Office 2007/Office 2010 (Word, Excel, et PowerPoint)	connexion web, WS-Federation (AD FS 2.0)
Lync 2010	WS-Federation (métadonnées) et WS-Trust (Assistant de connexion et AD FS 2.0)

4 Présentation de la configuration SSO et des éléments requis associés

Toutes les étapes d'installation qui doivent être effectuées pour installer la fonctionnalité d'authentification unique ainsi que les options associées sont disponibles et décrites sur Microsoft Online Portal (MOP).

Une fois authentifié, sur la page **Administration** MOP, sélectionnez **Utilisateurs** dans le volet gauche ou accédez à l'URL suivante : https://portal.microsoftonline.com/UserManagement/UserManager.aspx (éventuellement en anglais).

Le lien **En savoir plus** vous dirige sur la page Préparation à l'authentification unique[62] de la documentation en ligne. Les informations clés sont résumées dans la section ci-après.

Le lien **Activer** correspond à la page Configurer et gérer l'authentification unique (éventuellement en anglais)[63]. Cette page vous guide tout au long des 10 étapes de configuration de la fonctionnalité d'authentification unique (et de la synchronisation d'annuaires, qui n'est pas décrite dans ce document).

[62] Préparation à l'authentification unique : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/ff652540.aspx

[63] Configurer et gérer l'authentification unique : https://portal.microsoftonline.com/IdentityFederation/IdentityFederation.aspx

La page Authentification unique : étapes[64] fournit une vue d'ensemble de ces étapes.

4.1 Préparation de l'authentification unique

L'article Préparer l'authentification unique[65] décrit les opérations qui doivent être conduites afin de préparer l'environnement informatique local de l'organisation pour l'authentification unique et un déploiement réussi des identités fédérées. L'Active Directory local de l'organisation doit être configuré avec certains paramètres relatifs à la structure et à l'utilisation du nom de domaine Active Directory afin de fonctionner correctement pour l'authentification unique.

Pour préparer l'environnement Active Directory, nous recommandons d'exécuter l'outil d'aide au déploiement de Microsoft Office 365 pour les entreprises (éventuellement en anglais)[66] (*Office365DeploymentReadinessTool.exe*) fourni avec le guide de déploiement de Microsoft Office 365 (éventuellement en anglais)[67].

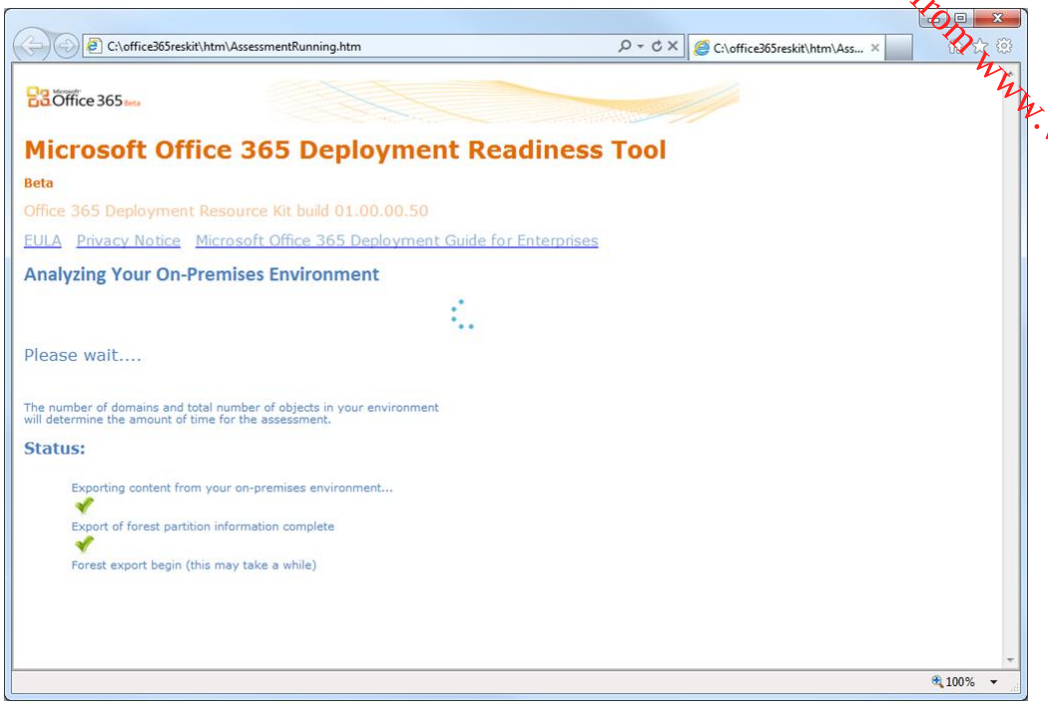
Cet outil inspecte l'environnement Active Directory et fournit un rapport contenant des informations qui indiquent si vous êtes prêt à configurer l'authentification unique. Si tel n'est pas le cas, il répertorie les modifications que vous devez apporter pour préparer l'authentification unique.

[64] AUTHENTIFICATION UNIQUE : ETAPES : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/hh125004.aspx

[65] Préparer l'authentification unique : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/ff652540.aspx

[66] Outil d'aide au déploiement de Microsoft Office 365 pour les entreprises : http://g.microsoftonline.com/0BD00en-US/506

[67] Guide de déploiement Microsoft Office 365 : http://community.office365.com/en-us/f/183/p/1541/5095.aspx#5095



Une évaluation pertinente doit comporter les rubriques suivantes :

1. **UPN :** les identités fédérées requièrent que les utilisateurs d'entreprise disposent d'un nom d'utilisateur principal (UPN), bien que ce ne soit pas le cas d'Active Directory. Les noms UPN associent les identités des utilisateurs dans Office 365 pour les entreprises avec les identités sur le nuage. Sans cette valeur, les utilisateurs ne sont pas en mesure de se connecter à Office 365 avec leurs informations d'identification d'entreprise.

   Les noms UPN qui sont utilisés pour les identités fédérées peuvent contenir des lettres, des chiffres, des points, des tirets et des traits de soulignement ; aucun autre type de caractère n'est autorisé. De plus, les noms UPN ne peuvent pas contenir un point avant le signe arobase (@). Afin de répondre aux problèmes de noms UPN, des options sont disponibles pour modifier les utilisateurs en bloc. Plusieurs outils peuvent être utilisés, tels que ADModify (éventuellement en anglais)[68].

   Correspondance des domaines : quand les noms de domaine Office 365 correspondent aux noms de domaine Active Directory local, aucun élément particulier n'est à prendre en compte en ce qui concerne l'espace de noms.

2. **Sous-domaines :** configurez en premier les domaines de premier niveau, puis les sous-domaines. Quand vous inscrivez votre domaine de premier niveau, tel que idmgt.fr, il est inutile d'enregistrer les sous-domaines, tels que legal.idmgt.fr ou paris.idmgt.fr. Les sous-domaines sont automatiquement enregistrés pour vous.

3. **Domaines locaux :** les domaines locaux qui sont configurés en tant que .local (par exemple, idmgt.local) ou .int (par exemple idmgt.int) ne peuvent pas être utilisés pour la fédération, car ils ne sont pas accessibles d'Internet (c'est-à-dire, ils ne sont pas accessibles par routage public ou identifiables dans le DNS). Vous pouvez enregistrer les domaines publics auprès du bureau d'enregistrement, puis fédérer ce domaine avec Office 365. Ensuite, vous ajoutez le nouveau domaine en tant que suffixe de domaine UPN à votre forêt, et spécifiez les noms

[68] ADModify : http://admodify.codeplex.com/

UPN sous le nouveau domaine. Cela permet que le suffixe de domaine UPN des utilisateurs fédérés se trouve sous le domaine que vous avez fédéré avec Office 365.

4. **Plusieurs domaines de connexion distincts** : jusqu'à présent, l'utilisation de plusieurs domaines de premier niveau pour les suffixes UPN des utilisateurs au sein d'une organisation (par exemple, @idmgt.fr ou @idmgt.co.uk) nécessitait le déploiement d'une instance séparée du service de fédération AD FS 2.0 pour chaque suffixe. Cela n'est désormais plus le cas après le package de correctifs cumulatifs 2 pour AD FS 2.0 (ou le package de correctifs cumulatifs 1 pour AD FS 2.0). (voir la section n° 4.3 INSTALLATION ET CONFIGURATION DU MODULE MICROSOFT ONLINE SERVICES).
5. **Plusieurs forêts :** plusieurs forêts ne sont pas actuellement prises en charge pour les identités fédérées.

4.2 Planification et déploiement d'AD FS 2.0

Comme précédemment indiqué, vous devez avoir une infrastructure AD FS 2.0 locale en place afin d'utiliser la fonctionnalité d'authentification unique d'Office 365 et d'authentifier les utilisateurs d'entreprise sur Office 365 à l'aide des identités fédérées. La section suivante décrit les différents scénarios d'implémentation AD FS 2.0 pour Office 365, afin que vous puissiez déterminer celui qui correspond le mieux à votre situation.

Nous recommandons la lecture de l'article Planifier et déployer AD FS 2.0 pour l'utilisation avec l'authentification unique[69] qui vous propose des éléments complémentaires pour vous guider dans votre choix.

4.2.1 Scénarios d'implémentation AD FS 2.0 pour Office 365

Comme avec la plupart des services d'entreprise, le service de fédération AD FS 2.0 peut être implémenté de différentes façons, selon vos besoins. Plus spécifiquement pour la fonctionnalité d'authentification unique d'Office 365, et comme décrit dans l'article Implication des scénarios d'implémentation AD FS 2.0 pour le service de fédération des identités Office 365 (éventuellement en anglais)[70], les scénarios d'implémentation AD FS 2.0 suivants décrivent comment le service de fédération AD FS 2.0 local est publié sur Internet.

Chaque scénario décrit peut être modifié en utilisant un serveur de fédération AD FS 2.0 autonome au lieu d'une batterie de serveurs. **Cependant, il est recommandé par Microsoft dans le cadre des meilleures pratiques que les services d'infrastructure critiques soient implémentés en utilisant une technologie de haute disponibilité pour éviter les pertes d'accès.**

La disponibilité du service de fédération AD FS 2.0 local affecte directement la disponibilité du service Office 365 pour les identités fédérées, et son niveau de service est de la responsabilité du client Office 365.

4.2.1.1 Scénario 1 - AD FS 2.0 totalement implémenté

Une batterie de serveurs de fédération AD FS 2.0 fournit les demandes clientes Active Directory via une seule authentification unique. Un serveur proxy de fédération AD FS 2.0 (à charge équilibrée) expose ces services d'authentification principaux à Internet en relayant les demandes et les réponses entre les clients Internet et l'environnement AD FS 2.0 interne.

---

[69] PLANIFIER ET DEPLOYER ACTIVE DIRECTORY FEDERATION SERVICES 2.0 POUR L'UTILISATION AVEC L'AUTHENTIFICATION UNIQUE : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/ff652539.aspx

[70] IMPLICATION DES SCENARIOS D'IMPLEMENTATION AD FS 2.0 POUR LE SERVICE DE FEDERATION DES IDENTITES OFFICE 365 : http://support.microsoft.com/kb/2510193

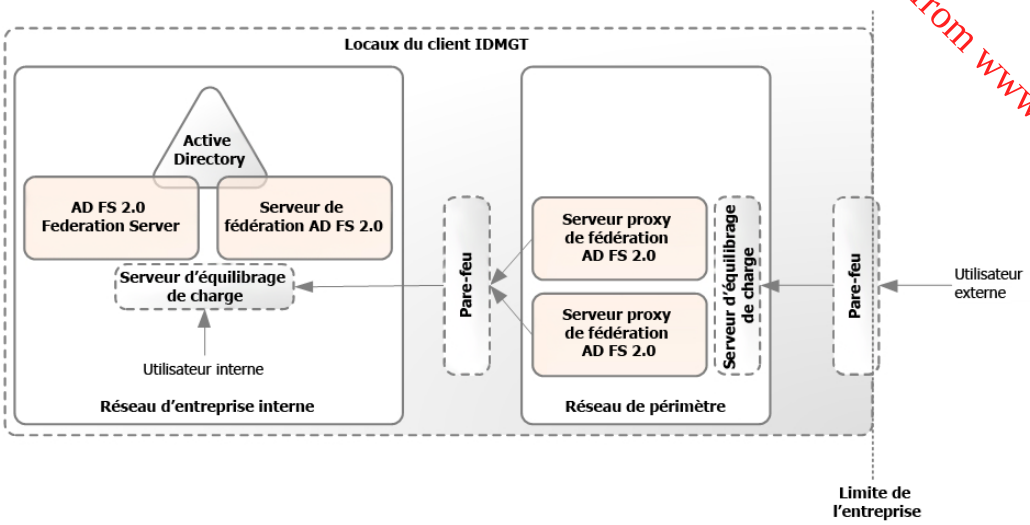


Figure 3Scénario d'implémentation AD FS 2.0 totalement implémenté

Dans la figure ci-dessus, vous pouvez voir que les utilisateurs d'entreprise sont dirigés vers le point de terminaison interne du serveur de fédération à charge équilibrée AD FS 2.0 mais que les utilisateurs externes devront utiliser le serveur proxy de fédération à charge équilibrée AD FS 2.0 pour accéder au service de fédération.

Il est à noter que, du point de vue d'Office 365, un proxy est utile aux utilisateurs externes afin de rediriger les demandes d'authentification client qui arrivent de l'extérieur du réseau d'entreprise vers la batterie de serveurs de fédération. Un tel proxy est en effet requis afin qu'Outlook (2007 ou 2010) puisse se connecter à Exchange Online à l'aide d'une identité fédérée. Sans un proxy, la création de profil Outlook demandera en permanence des informations d'identification (ou vous obtiendrez une réponse 401 HTTP).

Pour résumer, un proxy permet les scénarios utilisateur suivants :

1. **Ordinateur de travail, itinérance** : les utilisateurs qui ont ouvert une session sur des ordinateurs qui sont joints au domaine avec leurs informations d'identification d'entreprise, mais qui ne sont pas connectés au réseau d'entreprise (par exemple, un ordinateur de travail à la maison ou dans un hôtel), peuvent accéder aux services dans Office 365.
2. **Ordinateur personnel ou public** : quand l'utilisateur utilise un ordinateur qui n'est pas joint au domaine de l'entreprise, il doit se connecter avec ses informations d'identification d'entreprise pour accéder aux services dans Office 365.
3. **Smartphone** : sur un smartphone, pour accéder aux services dans Office 365, tels que Microsoft Exchange Online avec Microsoft Exchange ActiveSync, l'utilisateur doit se connecter avec ses informations d'identification d'entreprise.
4. **Microsoft Outlook ou autres clients de messagerie** : l'utilisateur doit se connecter à l'aide de ses informations d'identification d'entreprise pour accéder à sa messagerie Office 365 s'il utilise Outlook (2007 ou 2010) ou un client de messagerie qui ne fait pas partie d'Office ; par exemple un client IMAP ou POP.

Ce scénario d'implémentation est pris en charge par les services de support Office 365 et correspond à une meilleure pratique Microsoft. Ce scénario est la configuration optimale pour la plupart des organisations de sociétés de taille moyenne et grande. En fonction de la charge, des serveurs supplémentaires peuvent être nécessaires pour l'authentification. En prenant en compte les éléments ci-dessus, le déploiement AD FS 2.0 doit être mis à l'échelle pour répondre à toutes les demandes de service en ligne et pas uniquement le trafic Microsoft Online Portal (MOP), des portails SharePoint Online et Outlook Web Apps (OWA).

4.2.1.2 Scénario 2 - AD FS 2.0 publié via le pare-feu

Une batterie de serveurs de fédération AD FS 2.0 fournit les demandes clientes Active Directory via une seule authentification unique. Un serveur TMG (ou une batterie de serveurs) expose les services d'authentification principaux à Internet via proxy inversé.

> **Remarque importante :**
>
> *La Protection étendue pour l'authentification (EAP)[71] doit être désactivée sur la batterie de serveurs de fédération AD FS 2.0 pour que cela fonctionne, ce qui affaiblit le profil de sécurité du système, comme indiqué dans l'article Authentification impossible des ordinateurs clients Internet après la configuration d'Active Directory Federation Services (AD FS) DANS UNE CONFIGURATION « PUBLIEE VIA PARE-FEU » [72]. D'un point de vue de la sécurité, cela n'est pas recommandé.*

Afin que ce scénario soit pris en charge par les services de support Office 365, les conditions suivantes doivent être vraies :

- le proxy inversé du trafic HTTPS (port 443) entre le client Internet et le serveur de fédération doit être transparent ;
- le serveur de fédération doit recevoir une copie fidèle des demandes SAML du client Internet ;
- les clients Internet doivent recevoir des copies fidèles des réponses SAML comme si elles étaient directement attachées au serveur de fédération local.

L'article Dépannage des problèmes de disponibilité des services de fédération Active Directory lors de l'utilisation de Forefront Threat Management Gateway 2010[73] répertorie les problèmes de configuration courants qui peuvent faire échouer cette configuration.

4.2.1.3 Scénario 3 - AD FS 2.0 non publié

Une batterie de serveurs de fédération AD FS 2.0 traite les demandes client Active Directory via l'authentification unique, et la batterie de serveurs n'est pas exposée à Internet.

Les clients riches Outlook ne peuvent pas se connecter aux ressources Exchange Online comme décrit dans l'article Les utilisateurs fédérés ne peuvent pas se connecter à une boîte aux lettres Exchange Online[74]. La section n° 5.3 Présentation du flux d'authentification profil MEX/client riche fournit des explications supplémentaires sur ce problème.

De plus, les clients Internet (y compris les clients mobiles) ne peuvent pas utiliser les ressources Office 365. C'est pourquoi, pour des raisons de service, ce scénario n'est pas recommandé, car il ne fournit pas la suite complète des services qui sont pris en charge par la fonctionnalité d'authentification unique d'Office 365. Dans ces circonstances, ce scénario est tout de même pris en charge par les services de support d'Office 365.

Les administrateurs locaux doit régulièrement actualiser les données d'approbation de fédération manuellement en utilisant la commande **Update-MSOLFederatedDomain** de l'outil Module Microsoft Online Services pour Windows PowerShell (voir section n° 4.3.1 INSTALLATION DU MODULE MICROSOFT

---

[71] Protection étendue pour l'authentification : http://go.microsoft.com/fwlink/?LInkId=178431

[72] *Authentification impossible des ordinateurs clients Internet après la configuration d'Active Directory Federation Services (AD FS) dans une configuration « publiée via pare-feu »* : http://support.microsoft.com/kb/2535789

[73] DEPANNAGE DES PROBLEMES DE DISPONIBILITE DES SERVICES DE FEDERATION ACTIVE DIRECTORY LORS DE L'UTILISATION DE FOREFRONT THREAT MANAGEMENT GATEWAY 2010 : http://support.microsoft.com/kb/2535789

[74] LES UTILISATEURS FEDERES NE PEUVENT PAS SE CONNECTER A LA BOITE AUX LETTRES EXCHANGE ONLINE : http://support.microsoft.com/kb/2466333

ONLINE SERVICES). Pour plus d'informations, voir la section intitulée Mettre à jour les propriétés d'approbation[75] de l'article Vérifier et gérer l'authentification unique.

4.2.1.4 Scénario 4 - AD FS 2.0 publié via VPN

Une batterie de serveurs de fédération AD FS 2.0 (ou batterie de serveurs) traite les demandes client Active Directory via l'authentification unique, et le serveur ou la batterie de serveurs n'est pas exposé à Internet. Les clients Internet se connectent et utilisent le service de fédération AD FS 2.0 uniquement via une connexion de réseau privé virtuel (VPN) à l'environnement réseau local.

Sauf si les clients Internet (y compris les appareils mobiles) sont compatibles VPN, ils ne peuvent pas utiliser les services dans Office 365. Pour des raisons de qualité de service, cela n'est pas recommandé.

Afin que ce scénario soit pris en charge par les services de support Office 365, les conditions suivantes doivent être vraies :

- Le client peut se connecter au service de fédération AD FS avec le nom DNS via HTTPS (port 443).
- Le client peut se connecter aux points de terminaison Office 365 avec le nom DNS en utilisant les ports/protocoles appropriés.
- L'authentification unique pour les utilisateurs VPN/Internet est possible avec ce scénario, mais il n'est pas pris en charge.

En comparaison avec le scénario précédent, les administrateurs locaux doivent régulièrement actualiser les données d'approbation de fédération manuellement à l'aide de la commande **Update-MSOLFederatedDomain** de l'outil Microsoft Online Services pour Windows PowerShell (voir section n° 4.3.1 INSTALLATION DU MODULE MICROSOFT ONLINE SERVICES).

4.2.2 Création de l'infrastructure AD FS 2.0

En raison du nombre d'options de planification disponibles et des paramètres associés à prendre en compte, il n'est pas possible dans ce document de fournir un guide étape par étape de la création d'une infrastructure AD FS 2.0 ou de la modification d'une infrastructure existante.

En plus de l'article Planifier et déployer Active Directory Federation Services 2.0 pour l'utilisation avec l'authentification unique[76], vous pouvez consulter la documentation Microsoft TechNet Active Directory Federation Services (AD FS) 2.0 (éventuellement en anglais) pour des informations détaillées sur AD FS 2.0. Par exemple, l'article Installer le logiciel AD FS 2.0 (éventuellement en anglais)[77] fournit des instructions d'installation ainsi que des listes de contrôle pour de nombreuses options de planification. Si vous voulez utiliser le scénario « AD FS 2.0 totalement implémenté », vous ne pouvez pas installer et configurer l'option proxy tant que l'installation du service de fédération AD FS 2.0 n'est pas terminée.

Le package logiciel AD FS 2.0 (*AdfsSetup.exe*) peut être téléchargé à partir de *Active Directory Federation Services 2.0 RTW*[78]. Le correctif cumulatif 2 pour AD FS 2.0 doit être appliqué à tous les serveurs de fédération et proxy de fédération AD FS 2.0 déployés. Pour télécharger ce package, voir

[75] METTRE A JOUR LES PROPRIETES D'APPROBATION : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/ff652538.aspx#BKMK_UpdateTrustProperties

[76] PLANIFIER ET DEPLOYER ACTIVE DIRECTORY FEDERATION SERVICES 2.0 POUR L'UTILISATION AVEC L'AUTHENTIFICATION UNIQUE : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/ff652539.aspx

[77] INSTALLER LE LOGICIEL AD FS 2.0 : http://technet.microsoft.com/en-us/library/dd807096(WS.10).aspx

[78] Active Directory Federation Services 2.0 RTW : http://www.microsoft.com/fr-fr/download/details.aspx?id=10909

l'article 2681584 DESCRIPTION DU CORRECTIF CUMULATIF 2 POUR ACTIVE DIRECTORY FEDERATION SERVICES (AD FS) 2.0[79]

4.3 Installation et configuration du module Microsoft Online Services

Une fois l'infrastructure AD FS 2.0 créée en fonction du scénario d'implémentation choisi (voir section n° 4.2.1 Scénarios d'implémentation AD FS 2.0 pour Office 365), il est nécessaire d'installer l'outil Module Microsoft Online Services pour Windows PowerShell.

Remarque :

Cet outil a besoin de l'Assistant de connexion Microsoft Online Services (MSO SIA), qui est inclus dans l'application Configuration du bureau Office 365 ou disponible sous forme de téléchargement séparé : Assistant de connexion Microsoft Online Services pour les professionnels des technologies de l'information RTW[80].

L'exécution de cet outil ajoute un ensemble d'applets de commande à l'environnement et une interface PowerShell afin d'effectuer la configuration de la fonctionnalité d'authentification unique. Grâce aux applets de commande Windows PowerShell ajoutées, vous pouvez configurer l'approbation entre les domaines internes et la plateforme des identités Office 365. Cela permet aux demandes d'authentification des utilisateurs d'être redirigées vers l'URL de service de fédération AD FS 2.0.

Cela téléchargera également la clé publique pour le certificat utilisé pour la signature de jeton AD FS 2.0 et publiera les réclamations et les domaines à fédérer. Si la configuration AD FS 2.0 change, vous devrez la mettre à jour comme cela est expliqué plus loin dans ce document.

4.3.1 Installation du module Microsoft Online Services

Des privilèges d'administrateur sont nécessaires sur la session du serveur de fédération AD FS 2.0 pour installer le module Microsoft Online Services et pour configurer l'authentification unique.

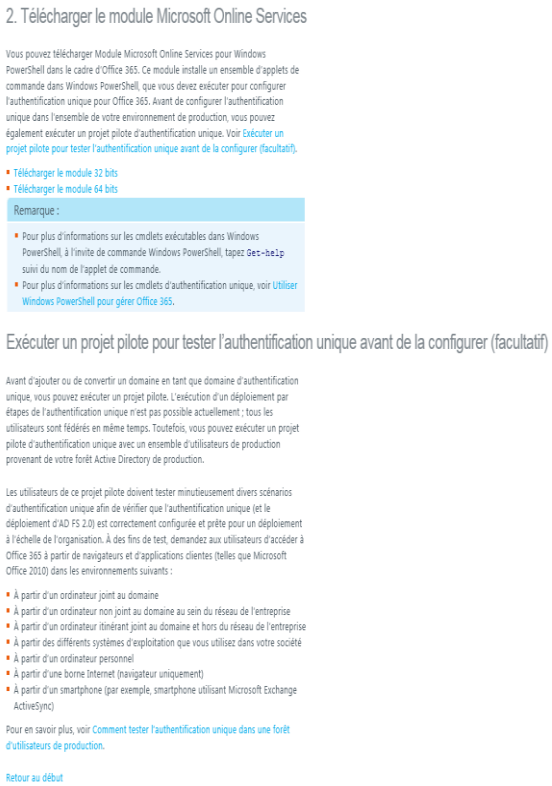
Pour installer l'outil, procédez ainsi :

1. À partir d'une session du serveur de fédération AD FS 2.0, ouvrez une session en tant qu'administrateur du domaine, naviguez sur le portail Microsoft Online Portal (MOP) jusqu'à l'étape 2 de la page INSTALLER ET CONFIGURER LE MODULE MICROSOFT ONLINE SERVICES POUR WINDOWS POWERSHELL POUR L'AUTHENTIFICATION UNIQUE[81].

[79] Article 2681584 DESCRIPTION DU CORRECTIF CUMULATIF 2 POUR ACTIVE DIRECTORY FEDERATION SERVICES (AD FS) 2.0 : http://support.microsoft.com/kb/2681584

[80] Assistant de connexion Microsoft Online Services pour les professionnels des technologies de l'information RTW : http://www.microsoft.com/fr-fr/download/details.aspx?id=28177

[81] INSTALLER ET CONFIGURER LE MODULE MICROSOFT ONLINE SERVICES POUR WINDOWS POWERSHELL POUR L'AUTHENTIFICATION UNIQUE : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/ff652560.aspx



2. Télécharger le module Microsoft Online Services

Vous pouvez télécharger Module Microsoft Online Services pour Windows PowerShell dans le cadre d'Office 365. Ce module installe un ensemble d'applets de commande dans Windows PowerShell, que vous devez exécuter pour configurer l'authentification unique pour Office 365. Avant de configurer l'authentification unique dans l'ensemble de votre environnement de production, vous pouvez également exécuter un projet pilote d'authentification unique. Voir Exécuter un projet pilote pour tester l'authentification unique avant de la configurer (facultatif).

- Télécharger le module 32 bits
- Télécharger le module 64 bits

Remarque :

- Pour plus d'informations sur les cmdlets exécutables dans Windows PowerShell, à l'invite de commande Windows PowerShell, tapez `Get-help` suivi du nom de l'applet de commande.
- Pour plus d'informations sur les cmdlets d'authentification unique, voir Utiliser Windows PowerShell pour gérer Office 365.

Exécuter un projet pilote pour tester l'authentification unique avant de la configurer (facultatif)

Avant d'ajouter ou de convertir un domaine en tant que domaine d'authentification unique, vous pouvez exécuter un projet pilote. L'exécution d'un déploiement par étapes de l'authentification unique n'est pas possible actuellement ; tous les utilisateurs sont fédérés en même temps. Toutefois, vous pouvez exécuter un projet pilote d'authentification unique avec un ensemble d'utilisateurs de production provenant de votre forêt Active Directory de production.

Les utilisateurs de ce projet pilote doivent tester minutieusement divers scénarios d'authentification unique afin de vérifier que l'authentification unique (et le déploiement d'AD FS 2.0) est correctement configurée et prête pour un déploiement à l'échelle de l'organisation. À des fins de test, demandez aux utilisateurs d'accéder à Office 365 à partir de navigateurs et d'applications clientes (telles que Microsoft Office 2010) dans les environnements suivants :

- À partir d'un ordinateur joint au domaine
- À partir d'un ordinateur non joint au domaine au sein du réseau de l'entreprise
- À partir d'un ordinateur itinérant joint au domaine et hors du réseau de l'entreprise
- À partir des différents systèmes d'exploitation que vous utilisez dans votre société
- À partir d'un ordinateur personnel
- À partir d'une borne Internet (navigateur uniquement)
- À partir d'un smartphone (par exemple, smartphone utilisant Microsoft Exchange ActiveSync)

Pour en savoir plus, voir Comment tester l'authentification unique dans une forêt d'utilisateurs de production.

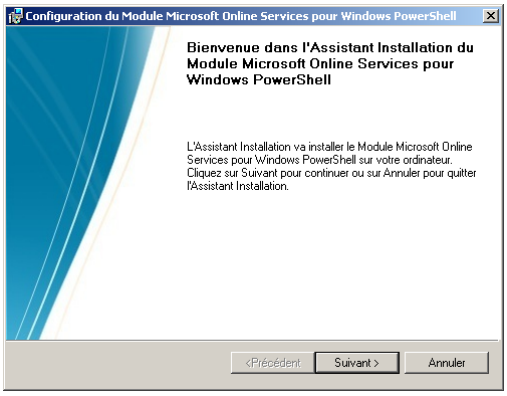
Retour au début

2. Cliquez sur le lien de téléchargement qui correspond à la version appropriée (32 bits ou 64 bits) du module Microsoft Online Services (*AdministrationConfig-fr.msi*) et cliquez sur **Exécuter** pour le lancer.

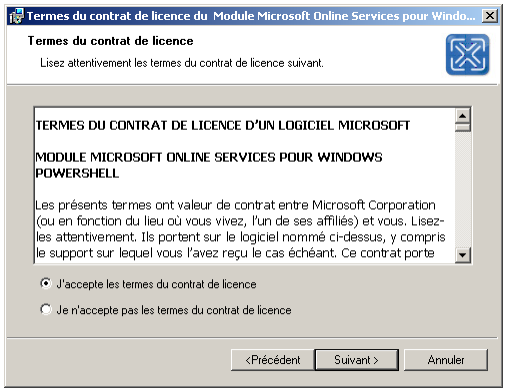
> **Remarque :**
>
> *Ce lien est également disponible sur la page Installer et gérer l'authentification unique (éventuellement en anglais)*[82] *dans la partie Administration de MOP sous la section Utilisateurs. Cette procédure de téléchargement a été décrite plus haut pour l'installation d'AD FS 2.0 et correspond à l'étape 3 du processus.*

L'Assistant **Installation du module Microsoft Online Services pour Windows PowerShell** s'ouvre.

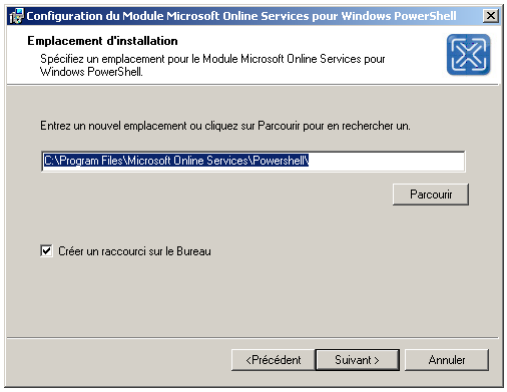
[82] INSTALLER ET GERER L'AUTHENTIFICATION UNIQUE : https://portal.microsoftonline.com/IdentityFederation/IdentityFederation.aspx



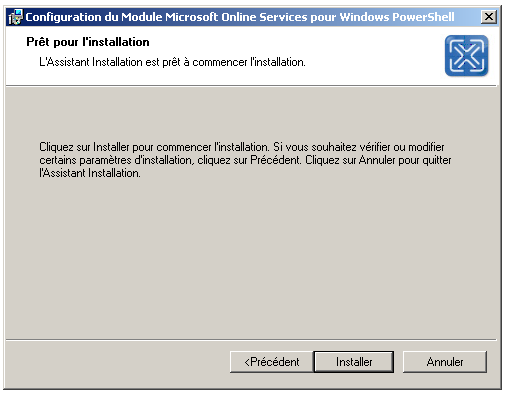
3. Sur la page **Bienvenue**, cliquez sur **Suivant**.



4. Sur la page **Termes du contrat de licence**, cliquez sur **J'accepte les termes du contrat de licence**, puis sur **Suivant**.



5. Sur la page **Emplacement d'installation**, sélectionnez l'emplacement par défaut et cliquez sur **Suivant**.



6. Sur la page **Prêt pour l'installation**, cliquez sur **Installer**.
7. Sur la dernière page, cliquez sur **Terminer**.

Comme décrit dans APPLETS DE COMMANDE WINDOWS POWERSHELL POUR OFFICE 365[83], les applets de commande suivantes effectuent les tâches liées à l'authentification unique (également appelée fédération des identités), telles que l'ajout d'un nouveau domaine d'authentification unique (également appelé domaine d'identité fédérée) à Office 365.

Tableau5 : Applets de commande d'authentification unique Windows PowerShell pour Office 365

Applet de commande d'authentification unique	Description
New-MsolFederatedDomain	Ajoute un nouveau domaine d'authentification unique à Office 365 et configure les paramètres d'approbation de la partie de confiance entre le service de fédération AD FS 2.0 local et Office 365. Étant donné les exigences de la vérification de domaine, vous devrez peut-être exécuter l'applet de commande plusieurs fois pour effectuer la procédure d'ajout d'un nouveau domaine d'authentification unique.
Convert-MsolDomainToStandard	Convertit le domaine spécifié à authentification unique en domaine à authentification standard. Ce processus permet également de supprimer les paramètres d'approbation de la partie de confiance du service de fédération AD FS 2.0 et d'Office 365. Après la conversion, cette applet de commande fait passer tous les utilisateurs existants de l'authentification unique à l'authentification standard. Tout utilisateur existant configuré pour l'authentification unique reçoit un nouveau mot de passe temporaire dans le cadre du processus de conversion. Tous les noms d'utilisateur convertis et tous les mots de passe temporaires sont enregistrés dans un fichier à des fins de référence pour l'administrateur. L'administrateur peut alors distribuer les nouveaux mots de passe temporaires aux utilisateurs convertis afin de leur permettre de se connecter à Office 365.

[83] APPLETS DE COMMANDE WINDOWS POWERSHELL POUR OFFICE 365 : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/hh125002.aspx

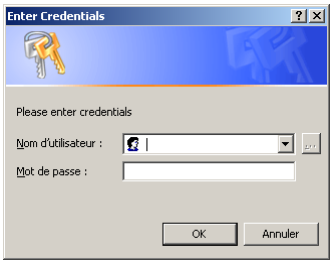
Applet de commande d'authentification unique	Description
Convert-MsolDomainToFederated	Convertit le domaine spécifié à authentification standard en domaine à authentification unique, et permet de configurer les paramètres d'approbation de la partie de confiance entre le service de fédération AD FS 2.0 et Office 365. Dans le cadre de la conversion d'un domaine à authentification standard en domaine à authentification unique, chaque utilisateur doit également être converti. Cette conversion se produit automatiquement à la prochaine connexion de l'utilisateur ; aucune action n'est requise par l'administrateur.
Get-MsolFederationProperty	Obtient les paramètres clés du service de fédération AD FS 2.0 et d'Office 365. Vous pouvez utiliser ces informations pour résoudre les problèmes d'authentification dus à des paramètres incohérents entre le service de fédération AD FS 2.0 et Office 365.
Get-MsolDomainFederationSettings	Obtient des paramètres clés d'Office 365. Utilisez l'applet de commande Get-MsolFederationProperty pour obtenir des paramètres pour Office 365 et le service de fédération AD FS 2.0.
Remove-MsolFederatedDomain	Supprime le domaine à authentification unique spécifié d'Office 365 et les paramètres d'approbation de la partie de confiance associés de AD FS 2.0. Remarque : Si des objets sont associés au domaine spécifié, vous ne pourrez pas supprimer le domaine.
Set-MsolDomainFederationSettings	Est utilisée pour mettre à jour les paramètres d'un domaine à authentification unique.
Set-MsolADFSContext	Définit les informations d'identification pour la connexion à Office 365 et au service de fédération AD FS 2.0. Cette applet de commande doit être exécutée avant d'appeler d'autres applets de commande d'authentification unique. Si cette applet de commande est appelée sans paramètre, l'utilisateur est invité à indiquer des informations d'identification pour se connecter aux différents systèmes. Quand le service de fédération AD FS 2.0 est utilisé à distance, l'utilisateur doit spécifier le nom de l'ordinateur sur le serveur AD FS 2.0 principal. Notez que le fichier journal spécifié est partagé par toutes les applets de commande d'authentification unique pendant la session. Un fichier journal par défaut est créé si aucun n'est spécifié.
Update-MsolFederatedDomain	Change les paramètres du service de fédération AD FS 2.0 et d'Office 365. Il est nécessaire d'exécuter cette applet de commande chaque fois que les URL ou informations de certificat changent dans AD FS 2.0 en raison de modifications apportées à la configuration ou de la maintenance régulière des certificats, notamment lorsqu'un certificat est sur le point d'expirer. Cette applet de commande doit également être exécutée lorsque des modifications se produisent dans Office 365. Pour confirmer que les informations sont correctes dans les deux systèmes, l'applet de commande Get-MsolFederationProperty peut être utilisée pour extraire les paramètres.

4.3.2 Connexion de Windows PowerShell à Microsoft Online Services

L'étape suivante consiste à ouvrir Windows PowerShell à partir du **module Microsoft Online Services pour Windows PowerShell** et à connecter Windows PowerShell au domaine en ligne à l'aide de vos informations d'identification d'administrateur en ligne.

- Pour connecter Windows PowerShell à Microsoft Online Services, procédez ainsi :

1. Cliquez sur **Démarrer** > **Tous les programmes > Microsoft Online Services > Module Microsoft Online Services pour Windows PowerShell** pour ouvrir une invite de commandes Windows PowerShell avec les applets de commande d'authentification unique.
2. À partir de l'invite de commandes Windows PowerShell, tapez **Connect-MsolService**. Cette commande vous demande vos informations d'identification d'administrateur Microsoft Online et définit le contexte de Windows PowerShell à administrateur en ligne.




```
PS C:\Windows\system32> Connect-MsolService
PS C:\Windows\system32> _
```

> **Remarque :**
>
> *Si une nouvelle version du module Windows PowerShell est disponible, un texte d'avertissement jaune vous indiquera qu'une version plus récente est disponible. Vérifiez toujours que vous exécutez la version la plus récente du module.*

3. Si vous ne vous trouvez pas sur un serveur AD FS 2.0, vous exécutez la commande **Set-MsolADFSContext** pour définir un serveur du contexte AD FS. Cette commande demande le nom d'hôte d'un serveur AD FS 2.0.

```
PS C:\Windows\system32> Set-MsolADFSContext

cmdlet Set-MsolADFSContext at command pipeline position 1
Supply values for the following parameters:
Computer: idmgt-dc
PS C:\Windows\system32> _
```

Vous N'avez PAS besoin d'exécuter cette applet de commande quand vous vous trouvez sur le serveur AD FS 2.0.

4.3.3 Création d'un nouveau domaine en tant que domaine fédéré

▶ Pour créer un nouveau domaine en tant que domaine fédéré à partir d'une invite de commandes Windows PowerShell, et après la connexion de Windows PowerShell à Microsoft Online Services, procédez ainsi :

1. Connectez Windows PowerShell à Microsoft Online Services (voir la section n° 4.3.2 CONNEXION DE WINDOWS POWERSHELL A MICROSOFT ONLINE SERVICES).
2. Exécutez la commande **New-MsolFederatedDomain –DomainName** <*nom domaine*>.

```
PS C:\Windows\system32> New-MsolFederatedDomain -DomainName demo.idmgt.archims.fr
WARNING: Please verify demo.idmgt.archims.fr domain owership by adding a DNS
demo.idmgt.archims.fr CNAME record targeting ps.microsoftonline.com at your
domain registrar. More information can be found
http://technet.microsoft.com/en-us/library/cc742578.aspx
PS C:\Windows\system32> _
```

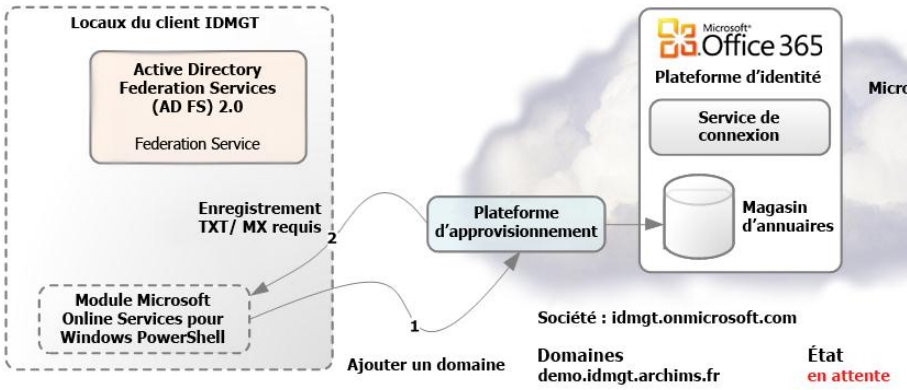


Figure 4Première exécution de l'applet de commande new-MsolFederatedDomain

3. Créez un enregistrement TXT de preuve de propriété de domaine (ou un enregistrement MX) pour le domaine qui est enregistré auprès du bureau d'enregistrement de noms de domaine, par exemple :

   Alias ou hôte : demo.idmgt.archims.fr
   Valeur : v=verifydomain MS=ms90115610
   TTL : 1 heure

   Office 365 utilise en effet un enregistrement DNS que vous créez auprès du bureau d'enregistrement de noms de domaine pour confirmer que vous êtes propriétaire du domaine. Pour plus d'informations, voir les articles Ajouter votre domaine à Office 365[84] et Vérifier un domaine auprès d'un bureau d'enregistrement de noms de domaine[85].

4. Exécutez la commande **New-MsolFederatedDomain –DomainName** <*nom domaine*> une seconde fois pour finaliser le processus une fois l'enregistrement de domaine créé.

```
PS C:\Windows\system32> New-MsolFederatedDomain –DomainName demo.idmgt.archims.fr
Successfully added demo.idmgt.archims.fr domain.
PS C:\Windows\system32> _
```

Cela vérifie la preuve de propriété du domaine. Le nouveau domaine enregistré est propagé sur les services Office 365 tels que Exchange Online :

- L'espace de noms réservé est « espace de noms fédéré » ;
- Le point de terminaison public du service de fédération AD FS 2.0 est défini pour chaque espace de noms à *https://adfs.demo.idemgt.archims.com/adfs/ls/*;
- Exchange Online crée le domaine enregistré en tant que Domaine accepté.

[84] AJOUTER VOTRE DOMAINE A OFFICE 365 : http://onlinehelp.microsoft.com/en-us/office365-enterprises/ff637620.aspx

[85] VERIFIER UN DOMAINE AUPRES D'UN BUREAU D'ENREGISTREMENT DE NOMS DE DOMAINE : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/gg584188.aspx

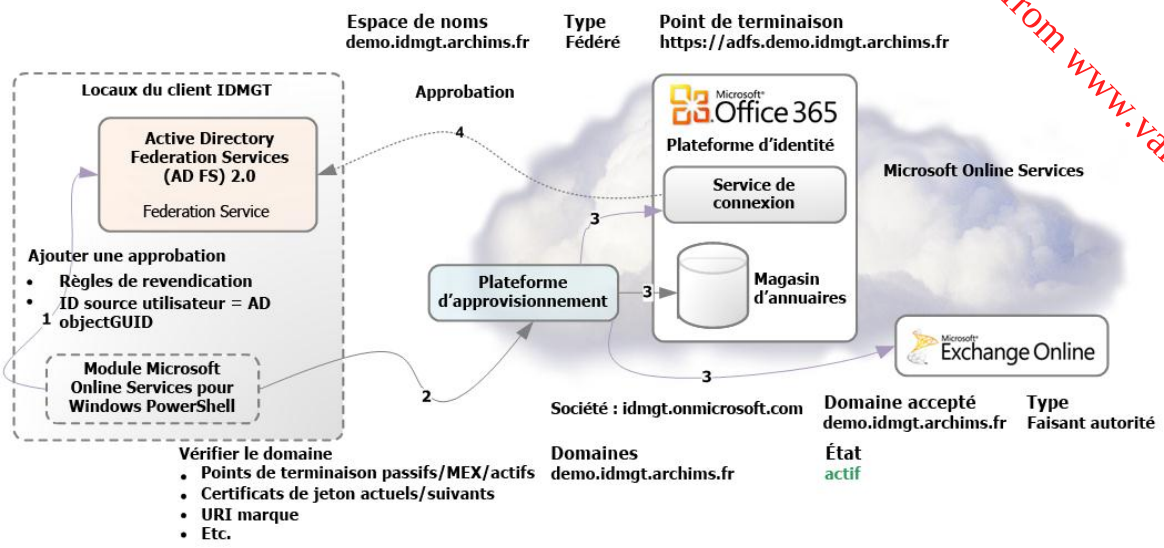


Figure 5Seconde exécution de l'applet de commande new-MsolFederatedDomain

> **Remarque :**
>
> *Le domaine peut également être ajouté à partir du portail Microsoft Online Portal (MOP). Les étapes sont les mêmes et le domaine doit également être vérifié de la même manière. Si le domaine a été ajouté via MOP, l'utilisateur devra convertir le domaine en domaine fédéré à partir de la ligne de commande, c'est pourquoi il est plus simple de le faire en une seule fois à partir de la ligne de commande. Les étapes de conversion d'un domaine sont décrites ci-après.*

Une fois les étapes ci-dessus effectuées, vous pouvez vérifier que le domaine a été correctement ajouté et est fédéré via Microsoft Online Portal (MOP). Quand vous êtes sur MOP, sélectionnez **Administrateur** dans la barre de navigation. Dans la colonne à gauche, sélectionnez **Domaines** sous **Gestion des utilisateurs**, puis sélectionnez le domaine que vous venez d'ajouter et vous constaterez qu'il est fédéré.

Quand le domaine est « fédéré », vous ne pourrez plus ajouter le suffixe de domaine aux comptes d'utilisateurs Microsoft Online. Les utilisateurs devront être créés localement afin que le nom de domaine fédéré leur soit disponible. Vous pouvez encore créer directement des comptes sur le nuage, mais le nom de domaine fédéré ne peut pas leur être assigné, sauf s'ils sont créés localement.

4.3.4 Mise à jour de modifications apportées à la configuration AD FS 2.0

Dans de nombreuses situations vous serez amenés à mettre à jour la plateforme des identités Office 365 avec de nouveaux paramètres du service de fédération AD FS 2.0.

Les métadonnées de fédération du service de fédération AD FS 2.0, telles qu'un certificat de signature de jeton, un nom de service de fédération et un identificateur de service de fédération, sont synchronisées avec la plateforme des identités Office 365 une fois lors de la conversion initiale du domaine locataire en domaine fédéré.

Si des métadonnées d'AD FS 2.0 changent localement, la relation d'approbation avec Office 365 peut être totalement rompue, ce qui peut provoquer des pannes à l'échelle de la société pour le locataire.

Vous trouverez ci-dessous une liste des problèmes courants qui entraîneront une mise à jour des informations si :

- le certificat SSL/TLS expire sur le(s) serveur(s) de fédération AD FS 2.0 et/ou le serveur proxy de fédération AD FS 2.0 (à charge équilibrée) (chaque année) ;
- un nouveau certificat est émis au(x) serveur(s) de fédération AD FS 2.0 et/ou serveur proxy de fédération AD FS 2.0 (à charge équilibrée) ;
- le scénario d'implémentation AD FS 2.0 a évolué (voir section n° 4.2.1 Scénarios d'implémentation AD FS 2.0 pour Office 365) ;
- l'URL d'un point de terminaison du service de fédération AD FS 2.0 a changé ;
- il existe des non correspondances avec le(s) certificat(s) ou la configuration elle-même. Les utilisateurs avec une identité fédérée peuvent obtenir l'erreur suivante lors de l'utilisation d'informations d'identification d'entreprise pour accéder à Office 365 : *« Un problème a été rencontré lors de l'accès au site. Essayez de naviguer sur le site de nouveau. »*
- Etc.

Pour corriger tous les problèmes, il est nécessaire que les informations locales soient cohérentes avec les informations de la plateforme des identités Office 365 et pour cela vous devrez mettre à jour les informations de configuration.

▶ Pour mettre à jour la configuration manuellement, procédez ainsi :

1. Connectez Windows PowerShell à Microsoft Online Services (voir la section 4.3.2 CONNEXION DE WINDOWS POWERSHELL A MICROSOFT ONLINE SERVICES).
2. Exécutez la commande **Update-MsolFederatedDomain –DomainName** <*nom domaine*>.

L'outil Microsoft Office 365 Federation Metadata Update Automation Installation (éventuellement en anglais)[86] peut être utilisé pour automatiser la mise à jour des métadonnées de fédération Microsoft Office 365 régulièrement pour s'assurer que les modifications apportées à la configuration du service de fédération AD FS 2.0 sont répliquées automatiquement sur la plateforme des identités Office 365.

Cet outil exécute une tâche planifiée, stockant de façon sécurisée les informations d'identification Microsoft Online (MSOL) dans le Gestionnaire d'informations d'identification sur un serveur AD FS 2.0,

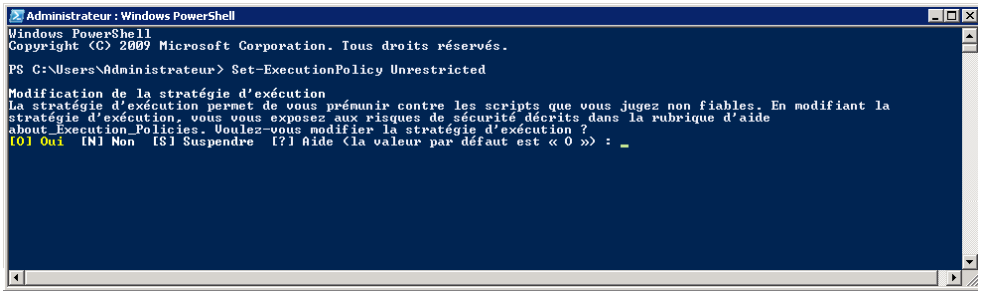
[86] Outil Microsoft Office 365 Federation Metadata Update Automation Installation : http://gallery.technet.microsoft.com/scriptcenter/Office-365-Federation-27410bdc

et envoie régulièrement les nouvelles métadonnées sur Office 365 pour éviter ou réduire les pannes dues à des modifications de métadonnées de production.

Pour mettre à jour la configuration automatiquement, procédez ainsi :

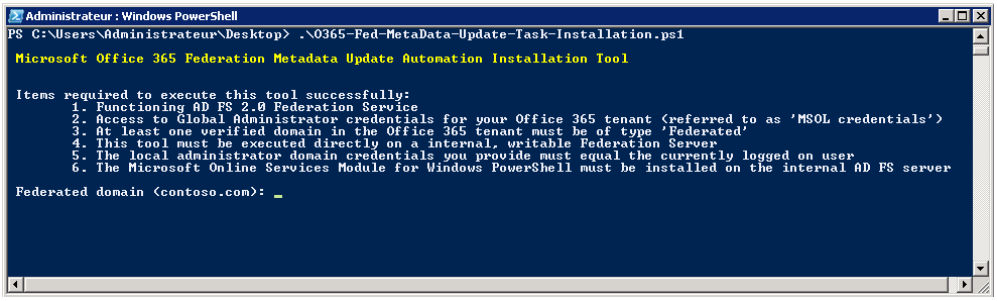
1. Ouvrez une session en tant qu'administrateur sur le serveur AD FS 2.0.
2. Téléchargez le fichier texte *O365-Fed-MetaData-Update-Task-Installation.ps1.txt* à partir de la galerie en ligne, et enregistrez-le en tant que fichier *.ps1* sur le bureau du serveur AD FS 2.0.
3. Cliquez avec le bouton droit sur le nouveau fichier créé *O365-Fed-MetaData-Update-Task-Installation.ps1*, cliquez sur **Propriétés**, **Débloquer** sous l'onglet **Général**, puis sur **OK**.
4. À partir du menu **Démarrer**, lancez une fenêtre d'administration Windows PowerShell, et modifiez le répertoire pour pointer vers le **Bureau**.
5. Exécutez la commande suivante et appuyez sur O afin d'exécuter les scripts sur le serveur :

```
PS C:\Users\Administrator> Set-ExecutionPolicy Unrestricted
```



6. Exécutez le fichier .ps1 enregistré à l'étape 2.

```
PS C:\Users\Administrator> cd .\Desktop
PS C:\Users\Administrator>.\O365-Fed-MetaData-Update-Task-Installation.ps1
```



7. Tapez et confirmez votre domaine fédéré, par exemple « *demo.idmgt.archims.fr* ».
8. Tapez votre compte d'administrateur global et votre mot de passe, par exemple :

   Nom d'utilisateur : admin@idmgt.onmicrosoft.com

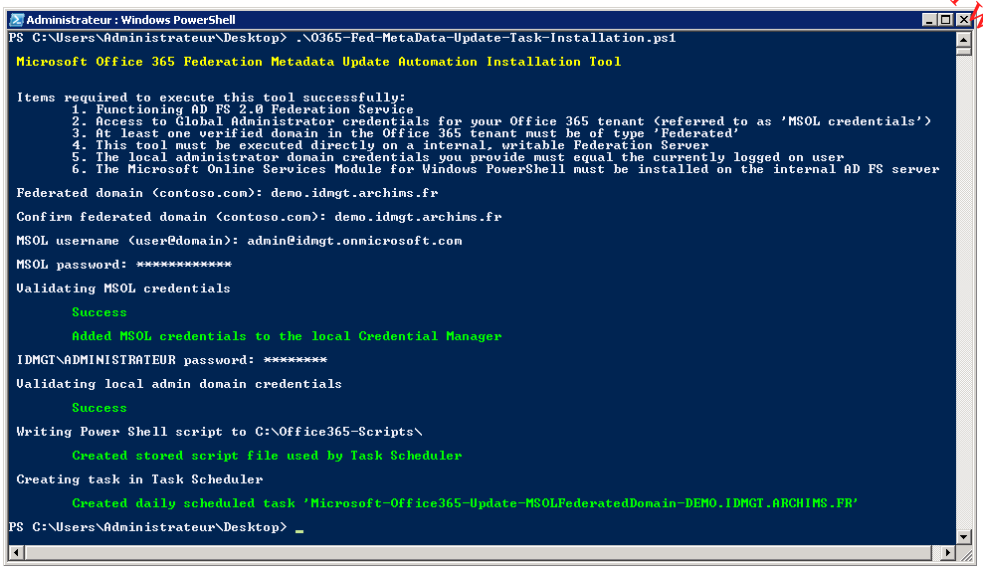
   Mot de passe : **********

   Si vous avez correctement tapé vos informations d'identification en ligne, le message suivant s'affiche :

   Success
   Added MSOL credentials to the local Credential Manager

9. Tapez le mot de passe pour l'administrateur actuellement connecté.

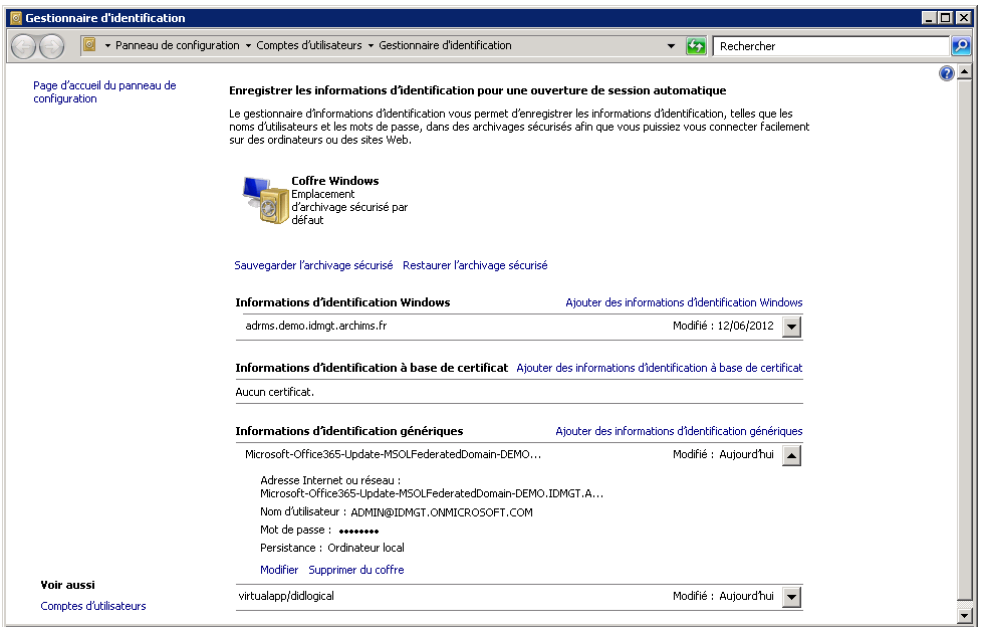
10. L'outil se poursuit jusqu'à la fin.



Les informations d'identification MSOL spécifiées sont stockées de façon sécurisée sur le serveur AD FS 2.0 afin que les applets de commande du module Microsoft Online Service pour Windows PowerShell puissent être exécutées sous la forme d'une tâche planifiée pour conserver les métadonnées entre le service de fédération local AD FS 2.0 et Office 365 synchronisées.

Pour afficher les informations d'identification MSOL, procédez ainsi :

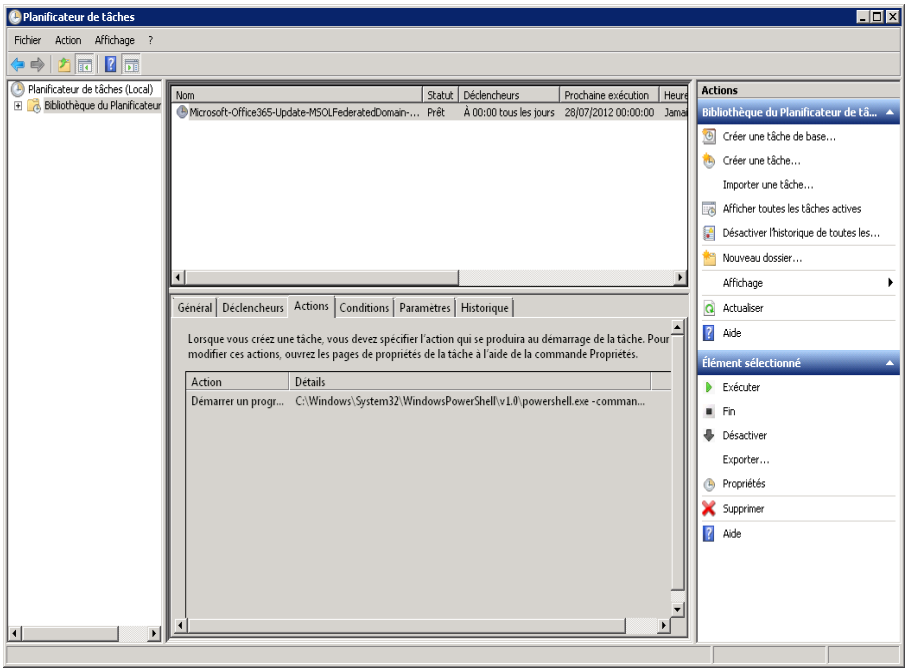
1. Cliquez sur **Démarrer**, tapez « *Credential* » dans le champ **Rechercher**, et cliquez dans les résultats sur **Gestionnaire d'informations d'identification**.
2. Les nouvelles informations d'identification génériques *Microsoft-Office365-Update-MSOLFederatedDomain-DEMO.IDMGT.ARCHIMS.FR* avec le nom d'utilisateur de l'administrateur global que vous avez tapées dans l'outil (*admin@idmgt.onmicrosoft.com*) s'affichent.



3. Fermez le **Gestionnaire d'identification**.

Pour afficher la tâche planifiée créée, procédez ainsi :

1. Cliquez sur **Démarrer**, tapez « *Task* » dans le champ **Rechercher**, puis cliquez dans les résultats sur **Planificateur de tâches**.
2. Sélectionnez **Bibliothèque du Planificateur de tâches** et affichez la tâche dans la liste nommée **Microsoft-Office365-Update-MSOLFederatedDomain-DEMO.IDMGT.ARCHIMS.FR**.



a. Cette tâche s'exécute chaque jour à minuit.
b. La tâche s'exécute sous le compte administrateur indiqué dans l'outil.
c. L'action qui s'exécute est la suivante :

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -command C:\Office365-Scripts\Microsoft-Office365-Update-MSOLFederatedDomain-DEMO.IDMGT.ARCHIMS.FR.ps1
```

3. Réduisez le **Planificateur de tâches**.
4. Accédez à *C:\Office365-Scripts*.
5. Remarquez le fichier .ps1 nommé *Microsoft-Office365-Update-MSOLFederatedDomain-DEMO.IDMGT.ARCHIMS.FR.ps1* et le fichier journal nommé *History.log*.
6. Ouvrez *History.log*, il contient l'emplacement d'installation de l'outil.

4.4 Vérification de l'authentification unique

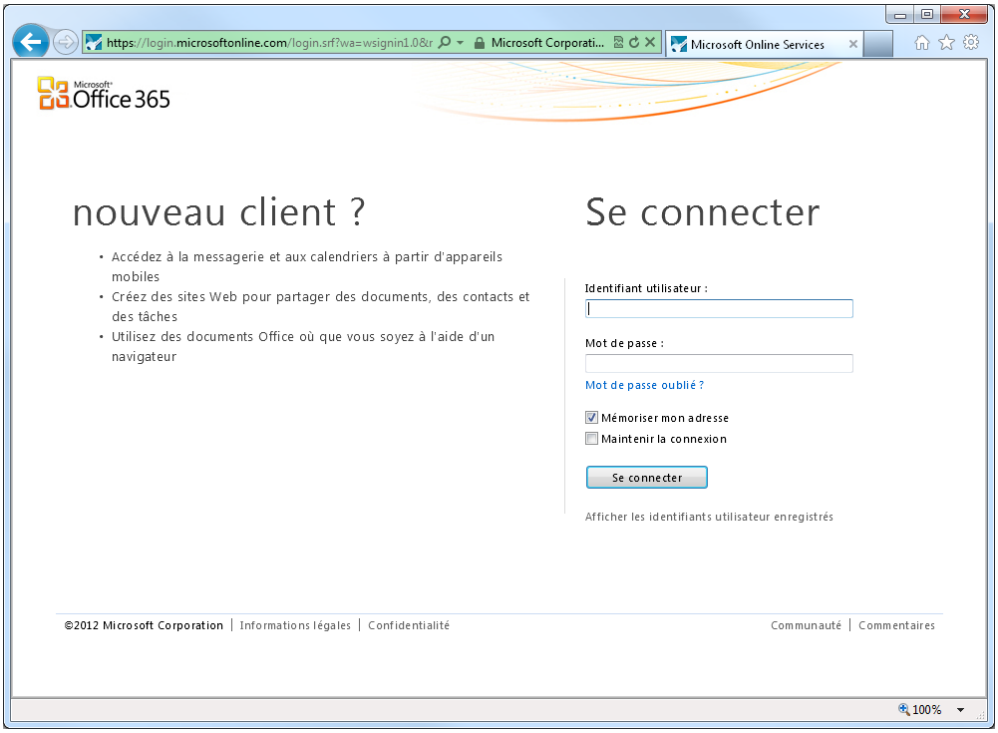
Comme suggéré dans l'article Vérifier et gérer l'authentification unique[87], il est recommandé de faire simple lors de la vérification (et/ou) du dépannage de l'authentification unique. Même si le problème rencontré concerne l'accès à Lync ou Exchange Online, il est conseillé d'accéder à Microsoft Online Portal (MOP) avec des informations d'identification locales pour vérifier si l'authentification unique fonctionne. Cela vous permet de vérifier si le problème est spécifique à l'application/au service ou s'il

[87] VERIFIER ET GERER L'AUTHENTIFICATION UNIQUE : http://onlinehelp.microsoft.com/fr-fr/office365-enterprises/ff652538.aspx

concerne l'authentification unique. Si l'utilisateur peut se connecter à MOP, mais ne peut pas se connecter à OWA avec ses informations d'identification d'entreprise, alors vous pouvez être certain que le problème n'est pas lié à l'authentification unique.

Pour vérifier l'authentification unique, procédez ainsi :

1. Ouvrez **Internet Explorer**, et tapez https://portal.microsoftonline.com pour accéder au portail Microsoft Online Portal (MOP). Vous êtes immédiatement redirigé vers l'URL login.microsoftonline.com qui est le fournisseur d'identité pour Microsoft Online Services.

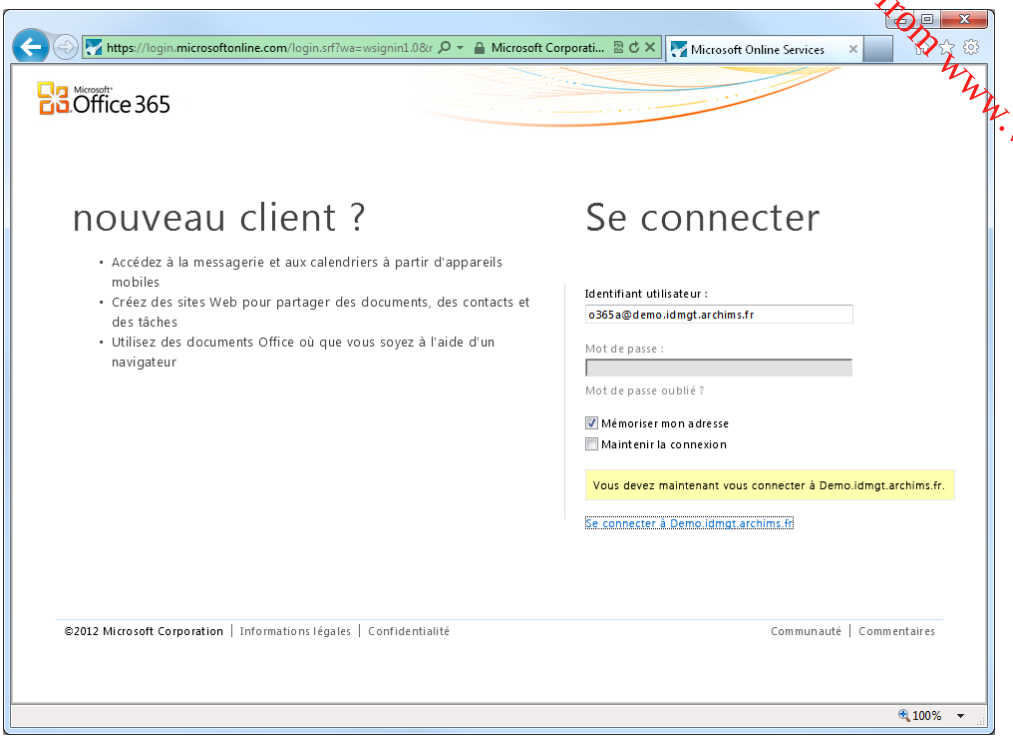


2. Tapez votre nom UPN d'entreprise local dans **Identifiant utilisateur**.
3. Cliquez dans la zone **Mot de passe**. Un processus HRD (home realm discovery) est déclenché pour les identités fédérées afin de savoir si la partie domaine du nom UPN est fédérée.

> **Remarque :**
>
> *Si vous avez activé le suivi HTTP dans IE ou si vous analysez le trafic via un outil tel que l'application de suivi HTTP Fiddler2 (éventuellement en anglais)[88], vous constatez que l'URL login.microsoftonline.com appelle GetUserRealm dans le cadre du processus HRD (home realm discovery). Vous noterez également des informations sur le point de terminaison passif du service de fédération AD FS 2.0 (voir section n° 5.1.5 POINTS DE TERMINAISON).*

4. Si l'authentification unique est correctement configurée, l'utilisateur ne peut pas taper son mot de passe. **Mot de passe** sera grisé. Un lien est fourni à l'utilisateur vers le service de fédération AD FS 2.0. Le message suivant s'affiche : « *Vous n'êtes pas obligé de vous connecter à <votre société>* ».

[88] Fiddler2 : http://www.fiddler.com



5. Cliquez sur le lien **Se connecter à <votre société>**, c'est-à-dire le lien **Se connecter à Demo.idmgt.archims.fr** dans la capture d'écran ci-dessus. Il s'agit d'un lien de redirection qui renvoie l'utilisateur au point de terminaison passif du service de fédération AD FS 2.0. L'utilisateur indique ses informations d'identification locales. Si l'utilisateur était connecté au domaine, le point de terminaison AD FS 2.0 serait atteint, mais sans l'invite des informations d'identification.

Si vous pouvez vous connecter, l'authentification unique a été correctement configurée.

.

5 Fonctionnement de l'authentification fédérée dans Office 365

Cette section fournit des informations supplémentaires sur la configuration définie via le module Microsoft Online Services pour Windows PowerShell afin de configurer l'authentification unique. Elle décrit les paramètres obtenus pour AD FS 2.0 ainsi que les différents types d'interaction entre les composants clés (le client, l'infrastructure AD FS 2.0 locale, la plateforme des identités 365 et son service de connexion), et les services dans Office 365.

5.1 Présentation de la configuration AD FS 2.0

5.1.1 Résumé du moteur et du pipeline des revendications AD FS 2.0

Comme précédemment indiqué, un service de fédération AD FS 2.0 est un STS qui se base sur un modèle de revendications. Dans ce modèle, le pipeline de revendications (voir Rôle du pipeline de revendications (éventuellement en anglais)[89]) représente le chemin que suivent les revendications jusqu'au service de fédération, avant de pouvoir être émises dans un jeton SAML.

Le service de fédération gère l'intégralité du processus de bout en bout du flux des revendications durant les étapes du pipeline, ce qui comprend le traitement des ensembles de règles de revendications par le moteur basé sur les règles de revendications (voir Rôle du moteur de revendications (éventuellement en anglais)[90]).

Le moteur de revendications gère trois tâches principales liées à une étape spécifique du pipeline de revendications :

1. l'acceptation des revendications entrantes provenant du fournisseur de revendications (**Règles de transformation d'acceptation**) ;
2. l'autorisation des demandeurs de revendications (**Règles d'autorisation d'émission**) ;
3. l'émission des revendications sortantes à une partie de confiance (**Règles de transformation d'émission**).

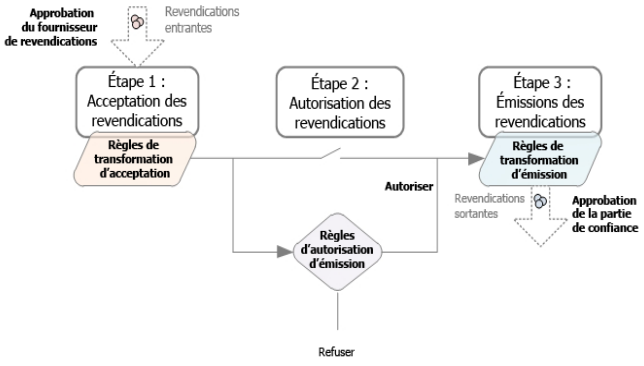


Figure 6Pipeline de revendications AD FS 2.0

[89] ROLE DU PIPELINE DE REVENDICATIONS : http://technet.microsoft.com/en-us/library/ee913585(WS.10).aspx

[90] ROLE DU MOTEUR DE REVENDICATIONS : http://technet.microsoft.com/en-us/library/ee913582(WS.10).aspx

En plus du moteur de revendications, qui traite les règles de revendications dans le cadre du pipeline, la configuration AD FS 2.0 dispose de trois relations principales pour contrôler la fonctionnalité :

1. **Magasin d'attributs** : le service de fédération AD FS 2.0 interroge les attributs afin d'obtenir la source des revendications. Si Active Directory Domain Services (AD DS) est déclaré par défaut, le service de fédération AD FS 2.0 peut également utiliser les attributs d'autres magasins, tels que Active Directory Lightweight Directory Services (AD LDS), des bases de données Microsoft SQL Server et d'autres sources de données.
2. **Approbation du fournisseur de revendications** : il s'agit de l'emplacement où l'approbation de fédération entre le service de fédération AD FS 2.0 et le fournisseur de revendications est configurée. Sur la base d'un ensemble de règles appelées **Règles de transformations d'acceptation**, les revendications du fournisseur de revendications sont filtrées par l'objet Approbation de la partie de confiance dans le contexte de la transaction. L'Active Directory local est le fournisseur de revendications pour l'authentification unique avec Office 365.
3. **Approbation de la partie de confiance** : il s'agit de l'emplacement où l'approbation de fédération entre le service de fédération AD FS 2.0 et la partie de confiance est configurée. Le service de fédération contrôle quels utilisateurs ont accès à la partie de confiance en fonction des **Règles d'autorisation d'émission**, puis il émet des revendications à la partie de confiance en fonction des **Règles de transformations d'émission**. La plateforme des identités Office 365 est la partie de confiance pour l'authentification unique avec Office 365. De même, dans Office 365, Exchange Online, SharePoint Online, etc. sont les parties de confiance de la plateforme des identités Office 365.

5.1.2 Descriptions des revendications

Le jeton de connexion SAML 1.1 émis par les services de fédération AD FS 2.0 à la partie de confiance de la plateforme des identités Office 365 contient les revendications qui proviennent du fournisseur de revendications Active Directory local (voir la section suivante) qui permet au service de connexion Office 365 de faire correspondre l'utilisateur à une identité fantôme sur le nuage :

- Le nom d'utilisateur principal (UPN) de l'utilisateur d'entreprise, qui est lié à la valeur configurée pour l'utilisateur grâce à la synchronisation d'annuaires.
- Un identificateur unique, rename-safe pour l'utilisateur, qui doit rester le même pour toute la durée de l'objet dans le nuage. Dans le cas contraire, cela peut créer des objets en double et des erreurs de synchronisation.

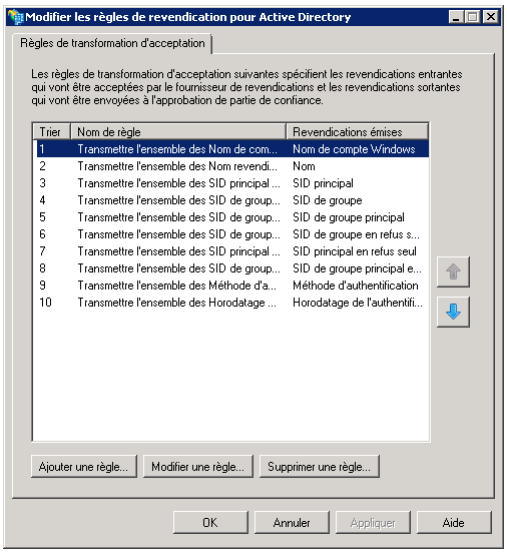
  Par défaut, il s'agit du GUID de l'objet Active Directory local (ImmutableID). Le ByteArray du GUID de l'objet est converti en chaîne Base64.

Il en résulte, dans ce cas précis, les 2 descriptions de revendications suivantes :

- UPN (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn).
- Source user ID (http://schemas.microsoft.com/LiveID/Federation/2008/08/ImmutableID).

5.1.3 Approbation de fournisseur de revendications Active Directory local

Les règles suivantes sont déclarées pour l'ensemble de **Règles de transformation d'acceptation** pour le magasin d'attributs Active Directory.



Les types de revendications entrantes sont les suivantes :

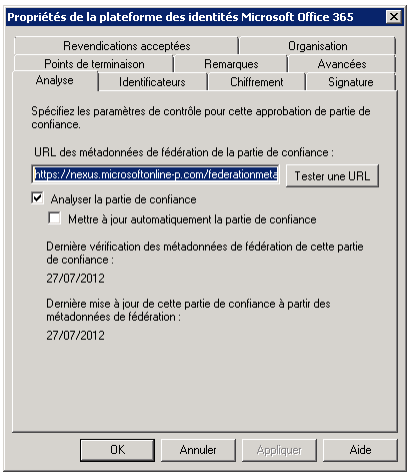
- Nom de compte Windows ;
- Nom ;
- SID principal ;
- SID de groupe ;
- SID de groupe principal ;
- Refuser uniquement SID de groupe ;
- Refuser uniquement SID de groupe principal ;
- Refuser uniquement SID de groupe ;
- Méthode d'authentification ;
- Heure d'authentification.

5.1.4 Approbation de partie de confiance de la plateforme des identités Microsoft Office 365

La création du domaine en tant que domaine fédéré avec les applets de commande du module Microsoft Online Services (voir section n° 4.3.3 Création d'un nouveau domaine en tant que domaine fédéré) provoque la définition automatisée d'une nouvelle approbation de partie de confiance de la plateforme des identités Microsoft Office 365.

5.1.4.1 Propriétés

L'onglet **Analyse** des **propriétés de la plateforme des identités Microsoft Office 365** affiche l'URL de laquelle les métadonnées du service de connexion Office 365 sont extraites : https://nexus.microsoftonline-p.com/federationmetadata/2007-06/federationmetadata.xml.



Cela prouve également que la définition d'approbation utilise la fonctionnalité AD FS 2.0 pour surveiller les métadonnées de la partie de confiance et pour mettre à jour automatiquement la définition d'approbation pour qu'elle reflète les paramètres actuels de la partie de confiance.

« Si la fédération est rompue. C'est PKI. Si ce n'est pas PKI, il y a une faute. Si vous avez tapé correctement (la casse est importante). C'est PKI »

Laura E. Hunter

Cela prend en charge de façon transparente toutes les modifications qui se produisent côté plateforme des identités Office 365. Cette fonctionnalité réduit les efforts d'administration nécessaires au maintient de l'approbation de la partie de confiance du côté du service de fédération AD FS 2.0.

De plus, il s'agit du rôle dédié à :

- l'applet de commande **Update-MsolFederatedDomain** du module Microsoft Online Services pour Windows Powershell pour mettre à jour manuellement

- ou -

- l'outil Microsoft Office 365 Federation Metadata Update Automation Installation pour mettre à jour automatiquement

les informations d'approbation (métadonnées de fédération), quand les informations sont modifiées du côté du service de fédération AD FS 2.0 et appliquer ces modifications à la plateforme des identités Office 365 (voir section n° 4.3.4 Mise à jour de modifications apportées à la configuration AD FS 2.0).

Les métadonnées du service de connexion Office 365 se présentent comme suit. La syntaxe générale et la sémantique des métadonnées sont définies dans OASIS Web Services Federation Language (WS-Federation) Version 1.2 (éventuellement en anglais)[91].

```
<?xml version="1.0" encoding="utf-8"?>
<EntityDescriptor wsu:Id="0c0d1ca7-7292-4bc6-801c-f880f6098f4e" entityID="urn:federation:MicrosoftOnline"
            xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
            xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <RoleDescriptor xsi:type="fed:SecurityTokenServiceType"
            protocolSupportEnumeration="http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis
            open.org/wsfed/federation/200706" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706">
    <KeyDescriptor use="signing" wsu:Id="stscer">
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
        <X509Data>
          <X509Certificate>MIICWzCCAcSgAwIBAgIJANswIPW/+LJFMA0GCSqGSIb3DQEBBQUAMCkxJzAlBgNV
                           BAMTHkxpdmUgSUQgU1RTIFNpZ25pbmcgUHVibGljIEtleTAeFw0xMDA3MTYyMTI0
                           NTZaFw0xNTA3MTUyMTI0NTZaMCkxJzAlBgNVBAMTHkxpdmUgSUQgU1RTIFNpZ25p
```

[91] OASIS WEB SERVICES FEDERATION LANGUAGE (WS-FEDERATION) VERSION 1.2 : http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf

```
                        bmcgUHVibGljIEtleTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAlM7mGMQ6
                        HaOJP8odYF4ArNF294zQzoRoR7PSv88tyHD/6wINeVn/ebD+XVI9ebRmRFdJYRFr
                        dqOrYwJOPmq9bG+zF2HblKX718BcAKw7Ku6iqkkOYwtCM1hijr9FlyBGIS9XoE+Y
                        y/qs+WNJyaUnXIwOYMwvojOevOKOtd6X7ekCAwEAAaOBijCBhzAdBgNVHQ4EFgQU
                        vODdCHPD3pifWehnZfE6eCztZj8wWQYDVR0jBFIwUIAUvODdCHPD3pifWehnZfE6
                        eCztZj+hLaQrMCkxJzAlBgNVBAMTHkxpdmUgSUQgU1RTIFNpZ25pbmcgUHVibGlj
                        IEtleYIJANswIPW/+LJFMAsGA1UdDwQEAwIBxjANBgkqhkiG9w0BAQUFAAOBgQBP
                        FFgHrWNtMRHsbjb/YUj67a7YvVnht11yH73oWLDdS/WW4VYHB3RiZuxUO7EtIFXk
                        yjRQ2lmHuza9+IljVKirLw8Zp6CH6tTiZC8WiyRI8cgenztPLO7x1Rwbg5d4bKkV
                        POdX7pe/Z6hrouK9Xc8828mjLO9OlyiH6L+tZcOhJw==
            </X509Certificate>
          </X509Data>
        </KeyInfo>
      </KeyDescriptor>
      <KeyDescriptor use="signing" wsu:Id="stsbcer">
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
          <X509Data>
            <X509Certificate>MIICWzCCAcSgAwIBAgIJAOAWPCFtWFILMA0GCSqGSIb3DQEBBQUAMCkxJzAlBgNV
                        BAMTHkxpdmUgSUQgU1RTIFNpZ25pbmcgUHVibGljIEtleTAeFw0xMDA3MTYyMTI0
                        MjZaFw0xNTA3MTUyMTI0MjZaMCkxJzAlBgNVBAMTHkxpdmUgSUQgU1RTIFNpZ25p
                        bmcgUHVibGljIEtleTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEArFszs9TG
                        9LSNOyT3PDzEMCql9OAN3qV6vv6HSoJR2E1WFZAXEt9KpO9AwVkDOpxat1DoCztf
                        dVlhk+ZhD8yv7x1PIzQJsLxC233Ch6pd3riFSJdAOBJtgr7vO7You6keKDj6hYWk
                        Io97zOFMbnR8GrJXxOaAR4bvwaF2osYjY3UCAwEAAaOBijCBhzAdBgNVHQ4EFgQU
                        m7Ph5zX8u1dUl8zE+5jQ+KarrUYwWQYDVR0jBFIwUIAUm7Ph5zX8u1dUl8zE+5jQ
                        +KarrUahLaQrMCkxJzAlBgNVBAMTHkxpdmUgSUQgU1RTIFNpZ25pbmcgUHVibGlj
                        IEtleYIJAOAWPCFtWFILMAsGA1UdDwQEAwIBxjANBgkqhkiG9w0BAQUFAAOBgQBd
                        aADu9GMezEPONs2wXMXZnwc3BAFWlP+hlp5T+vuVZlSsczyTn9Kmbw3oos8EMmro
                        GrzuxF3g71533ZnRC+Z+x1rltMXiI7vIcbwY1h3E6nt5X3/q/rhQu2bsCx7D9051
                        pCdWWSxjYHz2MH29x68OXOF0447aXyCzCg7O7Lj1cw==
            </X509Certificate>
          </X509Data>
        </KeyInfo>
      </KeyDescriptor>
      <fed:ClaimTypesOffered>
        <auth:ClaimType Uri="http://schemas.xmlsoap.org/claims/EmailAddress" Optional="True"
                        xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
          <auth:DisplayName>
            Email Address
          </auth:DisplayName>
        </auth:ClaimType>
        <auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2006/12/authorization/claims/action"
                        Optional="True" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
          <auth:DisplayName>
            Action for which the token is valid
          </auth:DisplayName>
        </auth:ClaimType>
        <auth:ClaimType Uri="http://schemas.microsoft.com/ws/2006/04/identity/claims/RequestorDomain"
                        Optional="True" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
          <auth:DisplayName>
            Domain name of the entity that requested the token on behalf of the user
          </auth:DisplayName>
        </auth:ClaimType>
        <auth:ClaimType Uri="http://schemas.microsoft.com/ws/2006/04/identity/claims/ThirdPartyRequested"
                        Optional="True" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
          <auth:DisplayName>
            Indicates this token was not requested directly by the user.
          </auth:DisplayName>
        </auth:ClaimType>
      </fed:ClaimTypesOffered>
      <fed:TokenTypesOffered>
        <fed:TokenType Uri="urn:oasis:names:tc:SAML:1.0"/>
      </fed:TokenTypesOffered>
      <fed:MexEndpoint>
        <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
          <Address>https://login.microsoftonline.com/login.srf</Address>
        </EndpointReference>
      </fed:MexEndpoint>
      <fed:PassiveRequestorEndpoint>
        <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
          <Address>https://login.microsoftonline.com/login.srf</Address>
        </EndpointReference>
      </fed:PassiveRequestorEndpoint>
    </RoleDescriptor>
```

```
    <RoleDescriptor xsi:type="fed:ApplicationServiceType"
                    protocolSupportEnumeration="http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-
                    open.org/wsfed/federation/200706" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"
                    xmlns:mfg="urn:microsoft:live:federation">
      <fed:TargetScopes>
        <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
          <Address>
            https://login.microsoftonline.com/extSTS.srf
          </Address>
        </EndpointReference>
      </fed:TargetScopes>
      <fed:ApplicationServiceEndpoint>
        <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
          <Address>
            https://login.microsoftonline.com/extSTS.srf
          </Address>
```

```
      </EndpointReference>
    </fed:ApplicationServiceEndpoint>
    <fed:PassiveRequestorEndpoint>
      <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
        <Address>
          https://login.microsoftonline.com/login.srf
        </Address>
      </EndpointReference>
    </fed:PassiveRequestorEndpoint>
    <mfg:FederationMetadataPutEPR>
      <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
        <Address>
          https://ppsanamespace.service.microsoftonline-p.net/pksecure/ProvisionTrustPK.srf
        </Address>
      </EndpointReference>
    </mfg:FederationMetadataPutEPR>
  </RoleDescriptor>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="#0c0d1ca7-7292-4bc6-801c-f880f6098f4e">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>aQPeWCSJOS22Dk60yhNDG/NCiIo=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>
        TCgu1tcOTAuJay2GEPFHlNbwJtXGX203/oEemOgToHNEE6IxOaXgRFduLNqZw/QMJdHgdXPf558E7+GmhQRRSfEiAyXkxQEoh
        Q7pvHgujapyo2iSTBgLIT7hme3nxADHvKrlEolKBIh3aBnTzOEqn1FUB68qvNH7UFuBqTUObjO=
    </SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509Certificate>
            MIICWzCCAcSgAwIBAgIJANswIPW/+LJFMAOGCSqGSIb3DQEBBQUAMCkxJzAlBgNVBAMTHkxpdmUgSUQgU1RTIFNpZ25pbm
            cgUHVibGljIEtleTAeFw0xMDA3MTYyMTI0NTZaFw0xNTA3MTUyMTI0NTZaMCkxJzAlBgNVBAMTHkxpdmUgSUQgU1RTIFNp
            Z25pbmcgUHVibGljIEtleTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAlM7mGMQ6Ha0JP8odYF4ArNF294zQzoRoR7
            PSv88tyHD/6wINeVn/ebD+XVI9ebRmRFdJYRFrdqOrYwJOPmq9bG+zF2HblKX718BcAKw7Ku6iqkkOYwtCM1hijr9FlyBG
            IS9XoE+Yy/qs+WNJyaUnXIwOYMwvoj0ev0KOtd6X7ekCAwEAAaOBijCBhzAdBgNVHQ4EFgQUvODdCHPD3pifwehnZfE6eC
            ztZj8wWQYDVR0jBFIwUIAUvODdCHPD3pifwehnZfE6eCztZj+hLaQrMCkxJzAlBgNVBAMTHkxpdmUgSUQgU1RTIFNpZ25p
            bmcgUHVibGljIEtleYIJANswIPW/+LJFMAsGA1UdDwQEAwIBxjANBgkqhkiG9w0BAQUFAAOBgQBPFFgHrWNtMRHsbjb/YU
            j67a7YvVnht11yH73oWLDdS/WW4VYHB3RiZuxUO7EtIFXkyjRQ2lmHuza9+IljVKirLw8Zp6CH6tTiZC8WiyRI8cgenztP
            LO7x1Rwbg5d4bKkVPOdX7pe/Z6hrouK9Xc8828mjLO9OlyiH6L+tZcOhJw==
        </X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
</EntityDescriptor>
```

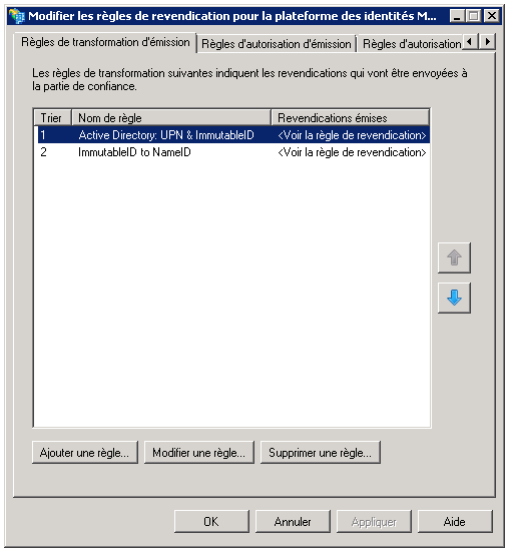
Le second élément **RoleDescriptor** correspond au rôle de partie de confiance du service de connexion Office 365 qui nous intéresse.

Cet élément définit 2 points de terminaison pour le service de connexion Office 365 pour l'interaction avec l'infrastructure locale de l'organisation :

1. un point de terminaison passif pour les clients web (navigateur) : https://login.microsoftonline.com/login.srf.
2. un point de terminaison actif pour les clients smart : https://login.microsoftonline.com/extSTS.srf.

5.1.4.2 Règles de transformation d'émission

La définition automatisée de l'approbation crée 2 règles personnalisées dans l'ensemble de **Règles de transformation d'émission**.



Ces 2 règles sont définies comme suit :

1. **Règle personnalisée « Active Directory: UPN & ImmutableID »** : En interrogeant Active Directory en fonction du nom de connexion utilisateur, cette règle extrait :

   - la revendication UPN : nom UPN de l'utilisateur lié à la valeur configurée pour l'utilisateur ;
   - la revendication ImmutableID : identificateur unique, rename-safe de l'utilisateur lié à la configuration de cet utilisateur.

   Cette règle permet d'utiliser comme source les éléments d'attribut UPN et ImmutableID de l'élément instruction de l'attribut dans le jeton de connexion SAML 1.1 émis come indiqué ci-après.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/claims/UPN",
"http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"), query =
"samAccountName={0};userPrincipalName,objectGUID;{1}", param = regexreplace(c.Value,
"(?<domain>[^\\]+)\\(?<user>.+)", "${user}"), param = c.Value);
```

2. **Règle personnalisée « ImmutableID to NameID »** : comme son nom l'indique, cette règle transforme la revendication ImmutableID en revendication SourceID.

   Cette règle permet d'utiliser comme source l'élément objet de l'élément instruction d'attribut dans le jeton de connexion SAML 1.1 émis comme indiqué ci-après.

```
c:[Type == "http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Value = c.Value, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified");
```

Le jeton de connexion SAML 1.1 obtenu est indiqué ci-dessous. Ce jeton signé XML est un jeton dit « de support » (un jeton de support avec une durée de vie courte, sans preuve de propriété), qui est émis par le service de fédération AD FS 2.0 pour le service de connexion Office 365.

Ce jeton comprend une instruction attribut et une instruction authentification :

- **Instruction attribut** : elle indique que le sujet identifié ici par un NameID (ImmutableID) est associé à certaines revendications (UPN et ImmutableID dans notre contexte). Les revendications sont fournies sous la forme d'une paire nom-valeur ;
- **Instruction authentification** : elle indique que le principal de sécurité (le sujet) a été authentifié par le service de fédération AD FS 2.0 à un moment donné à l'aide d'une méthode d'authentification spécifique : AuthenticationMethod=« urn:oasis:names:tc:SAML:1.0:am:password »;

La syntaxe générale et la sémantique des jetons SAML 1.1 sont définies dans la spécification principale de la norme OASIS SAML Assertions et protocoles pour OASIS Security Assertion Markup Language (SAML) V 1.1 (éventuellement en anglais)[92].

```
<saml:Assertion MajorVersion="1" MinorVersion="1" AssertionID="_55b4b481-da5e-49fa-a8f2-af3198cbd1b3"
                Issuer="http://sts.idmgt.demo/adfs/services/trust"
                IssueInstant="2012-02-14T15:53:38.976Z"
                xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
  <saml:Conditions NotBefore="2012-02-14T15:53:38.960Z" NotOnOrAfter="2012-02-14T16:53:38.960Z">
    <saml:AudienceRestrictionCondition>
      <saml:Audience>urn:federation:MicrosoftOnline</saml:Audience>
    </saml:AudienceRestrictionCondition>
  </saml:Conditions>
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
        jQs1n5ISOEKf4byoSsOr6A==
      </saml:NameIdentifier>
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod>
      </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Attribute AttributeName="UPN" AttributeNamespace="http://schemas.xmlsoap.org/claims">
      <saml:AttributeValue>o365a@demo.idmgt.archims.fr</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute AttributeName="ImmutableID"
                    AttributeNamespace="http://schemas.microsoft.com/LiveID/Federation/2008/05">
      <saml:AttributeValue>jQs1n5ISOEKf4byoSsOr6A==</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
  <saml:AuthenticationStatement AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password"
                                AuthenticationInstant="2012-02-14T15:53:38.929Z">
    <saml:Subject>
      <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
        jQs1n5ISOEKf4byoSsOr6A==
      </saml:NameIdentifier>
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod>
      </saml:SubjectConfirmation>
    </saml:Subject>
  </saml:AuthenticationStatement>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <ds:Reference URI="#_55b4b481-da5e-49fa-a8f2-af3198cbd1b3">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>hKJnVjG/rq/bdy1RrnztTIiBE6c=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
      tT4kMFkVL+l2D6fcD9QhDW+HN+rktCq7lZ9WMsPV+3ONoSq+KH/4qMrO0XncZySYlxMlhLbl7ZAJP5t0eErFbEBfH8+J3PPrsaRU+
      mXQe7lfIj1ir1l+hCpbC3HywnirmO1sLaj8NUHnM3/B0KDWblOzpPkOXKvM4Rd4SVsNiKykwp2Em3f8OhZWLu2mQRJxiti2n6NcOt
      Md4YhOV0fNhH5LHzc0SWNUiIALqtrc7b67YaOFMM21oxQBRffxnY4ns5kRU/aTKCTTwZzamBoRdCI97jOCjT8XTv+LfLHkcWaBH+5
      up0Xd+g3T8jTikGQpMDzuvbOtIlY69DUnCIzODQ==
    </ds:SignatureValue>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <X509Data>
        <X509Certificate>
          MIIC8DCCAdigAwIBAgIQF1RifzXrH59A+2Jtoe+5ADANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylBREZTIFNpZ25pbmcgL
```

[92] ASSERTIONS ET PROTOCOLES POUR OASIS SECURITY ASSERTION MARKUP LANGUAGE (SAML) V1.1 : http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf

```
            SBhZGZzLmRlbW8uaWRtZ3QuYXJjaGltcy5mcjAeFw0xMTA4MTAxOTIyNTZaFw0xMjA4MDkxOTIyNTZaMDQxMjAwBgNVBAMTKU
            FERlMgU2lnbmluZyAtIGFkZnMuZGVtby5pZG1ndC5hcmNoaW1zLmZyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE
            AwNpcxWSMJ3TbXfHEAAa4Moi7+S+k6JypSPq45FHAkyn3QkGzRsjJt9KF05/PvUsudukl+OZxXUHsb1pWMQniZAh5G7h6rUXf
            k1eeJhDHgBFpwI5yrLGdUlcGrQxNNE4UCLuDwRWG9WjA6Gr7q3bD68vFom/OitsyK18RRB4kCkFWHTln98b7EDieFOQPDxoRP
            o+Od6eQ/sejR6D7zJKW9LByT8H8BBOrm4CD9vpBoHiVxIgciLrARx0oCiayh/oYihZDWI8HYv1Tlvd9uh+Rxsax7QtUdWA/Me
            O6gOO5THo2YmxVA4wG3sdyl74MjgmPSv2qR6mP4GAGxk4sfK59iQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAxr2UPF+6osSL
            mF0bdn+Ysj98Q69c6LVLBmTcnd9VBqoefBtcvQe/rp34f2Ok3nqLVRgQv+aWfQrCwM5/5e93saZpdY2UH/U8cvSb+X2PqBK9y
            CPDejAtfjo3sCvOET+OUkoQirK4/CTnO7tg+37teZ1EVHaO3DHiI695llnW7Z7j/LH7TLaIP2l9WY2Fe5D+BOiZlYE9kCTDU9
            hVR4037cTKC7RKyl/hBPc1xRtQE0ya0lhb4THZjID4fHv9KYQOGaiUHnETt+Qc12pYnZW66O7KXj1Ap47IStGvWiOMbJ6jm4Y
            oGyZRa7MC5Gh2z3AQGZ2Rj1KPW3OQ/T3u3u84k
          </X509Certificate>
        </X509Data>
      </KeyInfo>
    </ds:Signature>
</saml:Assertion>
```

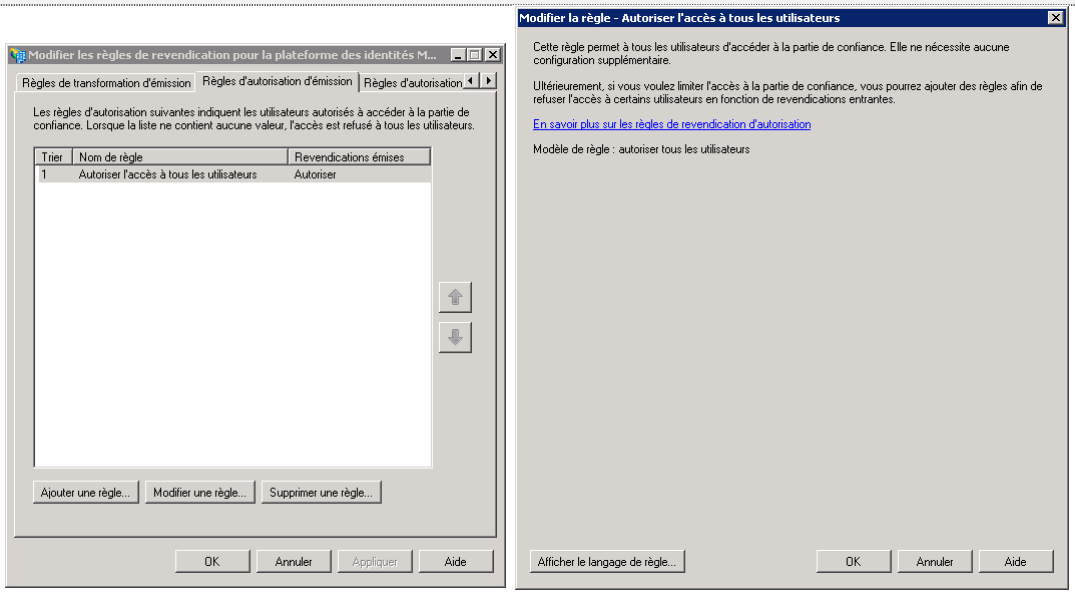

Il est à noter que l'URI émetteur, par exemple *http://sts.idmgt.demo/adfs/services/trust*, dans le jeton ci-dessus est utilisé pour localiser l'espace de noms dans le service de connexion Office 365.

5.1.4.3 Règles d'autorisation d'émission

La définition automatisée de l'approbation crée une règle « Permit Access to All Users » dans l'ensemble de **Règles d'autorisation d'émission**.

Cette règle qui autorise tous les utilisateurs est définie ainsi :

```
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");
```



5.1.5 Points de terminaison

Les points de terminaison AD FS 2.0 sont utilisés pour fournir aux clients l'accès aux solutions/applications fédérées. Les points de terminaison émettent des jetons d'authentification SAML aux clients, après la réussite de l'authentification client. Ces points de terminaison sont gérés sur le(s) serveur(s) de fédération (batterie) du service de fédération AD FS 2.0, et peuvent être gérés, sécurisés et publiés individuellement via un serveur proxy de fédération AD FS 2.0 (à charge équilibrée) (voir section n° 2.4.4.1 Serveur proxy de fédération AD FS 2.0).

Le serveur proxy de fédération AD FS 2.0 est un mode de déploiement d'AD FS 2.0 conçu spécialement dans le but de fournir un accès distant au service AD FS 2.0 hébergé en interne.

Dans un déploiement typique (voir section n° 4.2.1.1 Scénario 1 - AD FS 2.0 totalement implémenté), le serveur proxy de fédération est hébergé dans un réseau de périmètre, et transmet les données via le port 443 au FS (batterie), qui émet le jeton de sécurité SAML requis.

Le serveur proxy de fédération AD FS 2.0 peut répondre aux demandes de jeton d'accès aux parties de confiance AD FS 2.0. Il est à noter que, dans la mesure où le proxy ne concerne que le service AD FS 2.0, le serveur proxy de fédération ne peut pas accéder aux parties de confiance hébergées au sein du pare-feu d'entreprise sans l'aide d'un proxy inverse général, tel que Microsoft Forefront Threat Management Gateway (TMG).

De plus, dans le cadre de ce document, un serveur proxy de fédération AD FS 2.0 est requis pour Exchange Online, ainsi que pour permettre l'accès à SharePoint 2010 Online et Lync Online en dehors du réseau d'entreprise interne comme indiqué précédemment. De plus, le service de fédération AD FS 2.0 au sein du réseau d'entreprise et le serveur proxy de fédération AD FS 2.0 doivent être implémentés pour une haute disponibilité, car une panne de l'infrastructure empêchera l'accès au service de fédération.

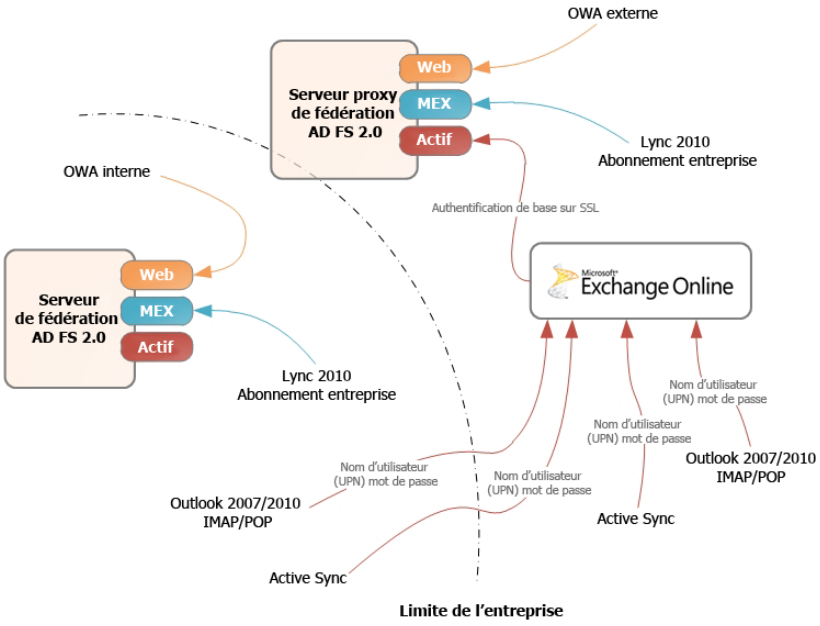


Figure 7Points de terminaison AD FS 2.0

Pour accéder aux services en ligne Office 365, trois points de terminaison distincts doivent être considérés :

1. **Point de terminaison de fédération passif (WS-Fed Passive Profile)** : Ce point de terminaison est utilisé par les clients web, lors de l'accès aux services suivants : Microsoft Online Portal (MOP), portails SharePoint Online, Outlook Web Apps (OWA).

   Le client web (navigateurs) s'authentifie directement avec le service de fédération AD FS 2.0, via ce point de terminaison

   En raison d'une transition en interactions de navigateur pendant l'authentification, ce point de terminaison s'applique également à Office 2007 Service Pack 2 (SP2) ou Office 2010 (Word, Excel ou PowerPoint) lors de l'ouverture de documents à partir d'une bibliothèque de documents SharePoint Online. Le client compte sur une réponse de SharePoint Online pour présenter une fenêtre de boîte de dialogue de navigateur qui prend en charge les protocoles web de fédération (WS-Fed dans ce cas) qui s'appuient sur les schémas de redirection.

   Le flux d'authentification qui utilise ce point de terminaison est décrit dans la section n° 5.2 Présentation du flux d'authentification profil passif/web.

2. **Point de terminaison de fédération actif (WS-Trsut Active Profile)** : Ce point de terminaison est utilisé par les clients riches qui prennent en charge AD FS 2.0 et spécifiquement par Lync 2010 et le client d'abonnement Office dans le cadre de ce document.

   Les deux clients indiqués ci-dessous négocient l'authentification directement avec le service AD FS 2.0, via ce point de terminaison. Ce flux d'authentification est décrit dans la section n° 5.3 Présentation du flux d'authentification profil MEX/client riche.

3. **Point de terminaison profil authentification de base/active EAS** : Ce point de terminaison s'applique à tous les clients qui ont besoin d'un service pour s'authentifier au nom des utilisateurs, et qui utilisent pour cela l'authentification de base (informations d'identification passées via l'authentification de base).

   Pour Office 365, ce point de terminaison est utilisé par Microsoft Exchange 2010 ActiveSync (EAS), Outlook 2007 et 2010, IMAP, POP et SMTP, Exchange 2010 Web Services.

   Le client envoie des informations d'identification de base sur SSL à Exchange Online et Exchange Online transmet cette demande d'authentification par proxy au service de fédération AD FS 2.0 au nom du client, via ce point de terminaison. Ce flux d'authentification est décrit dans la section n° 5.4 Présentation du flux d'authentification profil authentification de base/active EAS.

Pour des raisons de limitations d'accès client, ces trois points de terminaison peuvent être contrôlés/filtrés au niveau du serveur proxy de fédération (s'il existe, en fonction du scénario d'implémentation choisi, voir section n° 4.2.1 Scénarios d'implémentation AD FS 2.0 pour Office 365). De plus, le filtrage via des règles d'émission AD FS 2.0 est également pris en charge depuis octobre 2011 (voir section n° 6.3 Limitation de l'accès aux services Office 365 en fonction de l'emplacement du client).

L'applet de commande **Get-MsolFederationProperty** permet d'afficher les informations de point de terminaison AD FS 2.0 actuel.

Pour afficher les paramètres actuels, procédez ainsi :

1. Connectez Windows PowerShell à Microsoft Online Services (voir la section n° 4.3.2 CONNEXION DE WINDOWS POWERSHELL A MICROSOFT ONLINE SERVICES).
2. Exécutez la commande **Get-MsolFederationProperty –DomainName** <*nom domaine*>. Le résultat de la commande ci-dessus est indiqué ci-après. Ces informations sont très utiles et peuvent être utilisées pour vérifier rapidement des problèmes de configuration de l'authentification unique.

```
PS C:\Windows\system32> Get-MSOLFederationProperty -DomainName demo.idmgt.archims.fr

Source                       : ADFS Server
ActiveClientSignInUrl        : https://adfs.demo.idmgt.archims.fr/adfs/services/trust/2005/usernamemixed
FederationServiceDisplayName : ADFS IDMGT MTC Paris
FederationServiceIdentifier  : http://sts.idmgt.demo/adfs/services/trust

FederationMetadataUrl        :
https://adfs.demo.idmgt.archims.fr/adfs/services/trust/mexPassiveClientSignInUrl       :
PassiveClientSignOutUrl      :
                               [Issuer]
                                 CN=ADFS Signing - adfs.demo.idmgt.archims.fr
                               [Serial Number]
                                 1754627F35EB1F9F40FB626DA1EFB900
                               [Not Before]
                                 10/08/2011 21:22:56
                               [Not After]
                                 09/08/2012 21:22:56
                               [Thumbprint]
                                 25A70E3841C2614B097587EBDB9BBF0AE00D818C
NextTokenSigningCertificate  :
Source                       : Microsoft Office 365
ActiveClientSignInUrl        :
https://adfs.demo.idmgt.archims.fr/adfs/services/trust/2005/usernamemixedFederationServiceDisplayName : ADFS
IDMGT MTC Paris
FederationServiceIdentifier  : FederationMetadataUrl        :
PassiveClientSignInUrl       :
                               [Issuer]
                                 CN=ADFS Signing - adfs.demo.idmgt.archims.fr
```

```
                              [Serial Number]
                                1754627F35EB1F9F40FB626DA1EFB900
                              [Not Before]
                                10/08/2011 21:22:56
                              [Not After]
                                09/08/2012 21:22:56
                              [Thumbprint]
                                25A70E3841C2614B097587EBDB9BBF0AE00D818C
NextTokenSigningCertificate  :
```

Cela indique les informations de point de terminaison du service de fédération AD FS 2.0 suivantes :

- le point de terminaison de fédération passif (WS-Fed Passive Profile) est le point de terminaison *adfs/ls/*, qui correspond à l'entrée **PassiveClientSignInUrl** ;
- le point de terminaison de fédération actif (WS-Trust Active Profile) est le point de terminaison */adfs/services/trust/mex/* , qui correspond à l'entrée **FederationMetadataUrl** .
- Le point de terminaison profil authentification de base/active EAS est le point de terminaison */adfs/services/trust/2005/usernamemixed*, qui correspond à l'entrée **ActiveClientSignInUrl** .

Si, pour une raison quelconque, un client utilise un point de terminaison incorrect, cette commande peut être exécutée pour savoir pourquoi.

Pour le dépannage, et comme décrit dans les sections suivantes, le flux d'authentification des communications d'authentification unique Office 365 est prévisible. Le flux d'authentification attendu peut être comparé à une capture du flux d'authentification réel qui a eu lieu lors d'une tentative d'authentification unique qui a échoué afin de déterminer où le problème se pose.

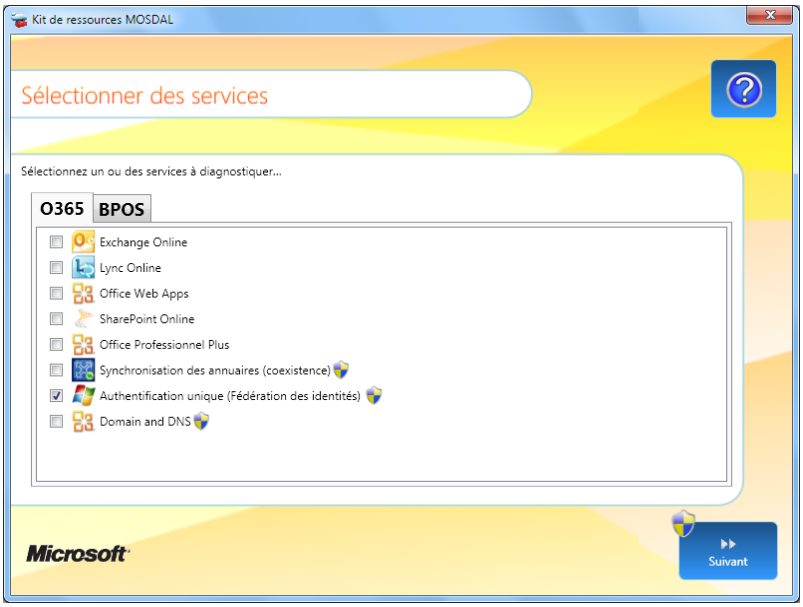
La partie Diagnostic d'authentification AD FS du Kit de ressources de support Microsoft Online Services Diagnostics and Logging (MOSDAL) 4.0[93] peut réaliser cette capture et cette comparaison afin de dépanner les problèmes d'authentification fédérée passive/active avec Office 365 en :

- détectant si l'ordinateur se trouve sur le réseau d'entreprise ou sur Internet ;
- vérifiant l'enregistrement d'Office 365 ;
- vérifiant que les métadonnées MEX/Federation peuvent être extraites du service de fédération AD FS 2.0 ;
- effectuant une connexion active/passive à Office 365 à l'aide du jeton de connexion AD FS 2.0 émis.

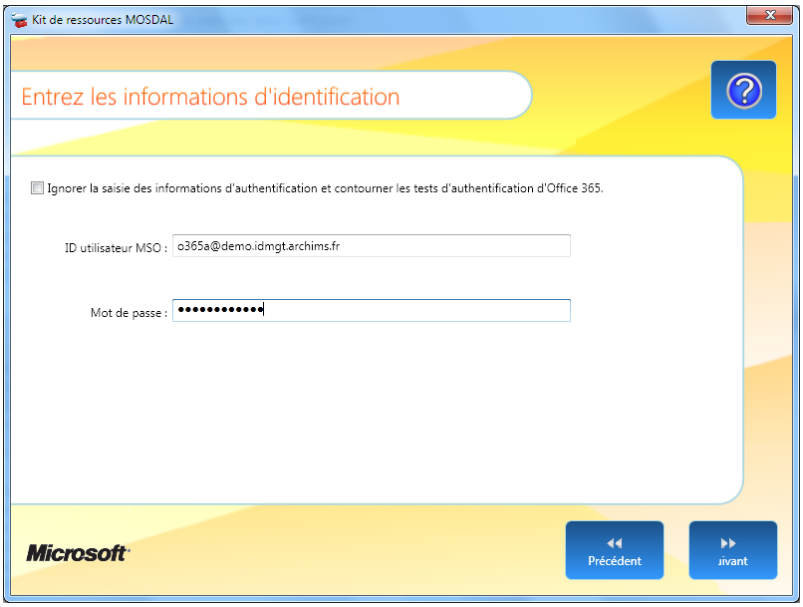
Pour exécuter MOSDAL pour tester l'authentification unique passive/active, procédez comme suit :

1. Téléchargez le package .msi à partir du Centre de téléchargement Microsoft et installez-le.
2. Lancez le **Kit de ressources de support MOSDAL**.

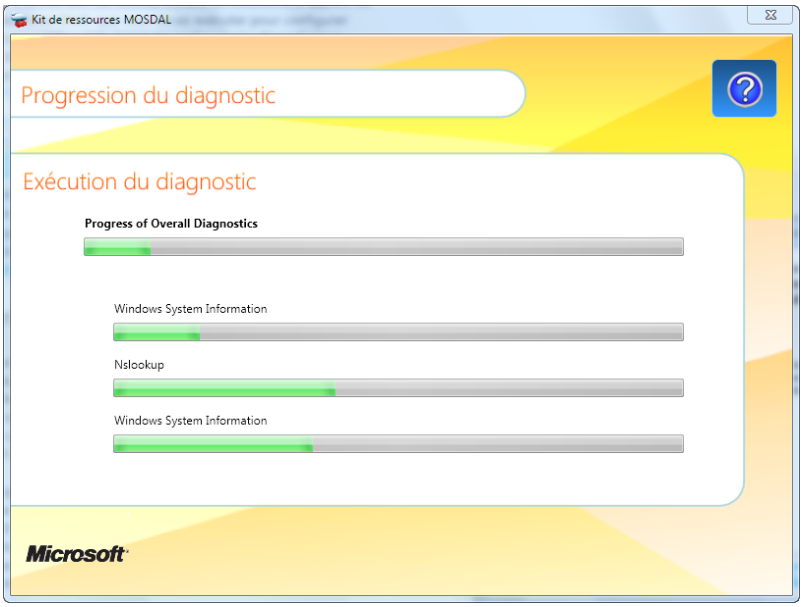
[93] Kit de ressources de support Microsoft Online Services Diagnostics and Logging (MOSDAL) 4.0 : http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=626



3. Sous l'onglet **O365**, sélectionnez **Authentification unique (Fédération des identités)**, puis cliquez sur **Suivant**.



4. Tapez vos informations d'identification, puis cliquez sur **Suivant**.
5. Cliquez sur **Suivant** pour démarrer les diagnostics.

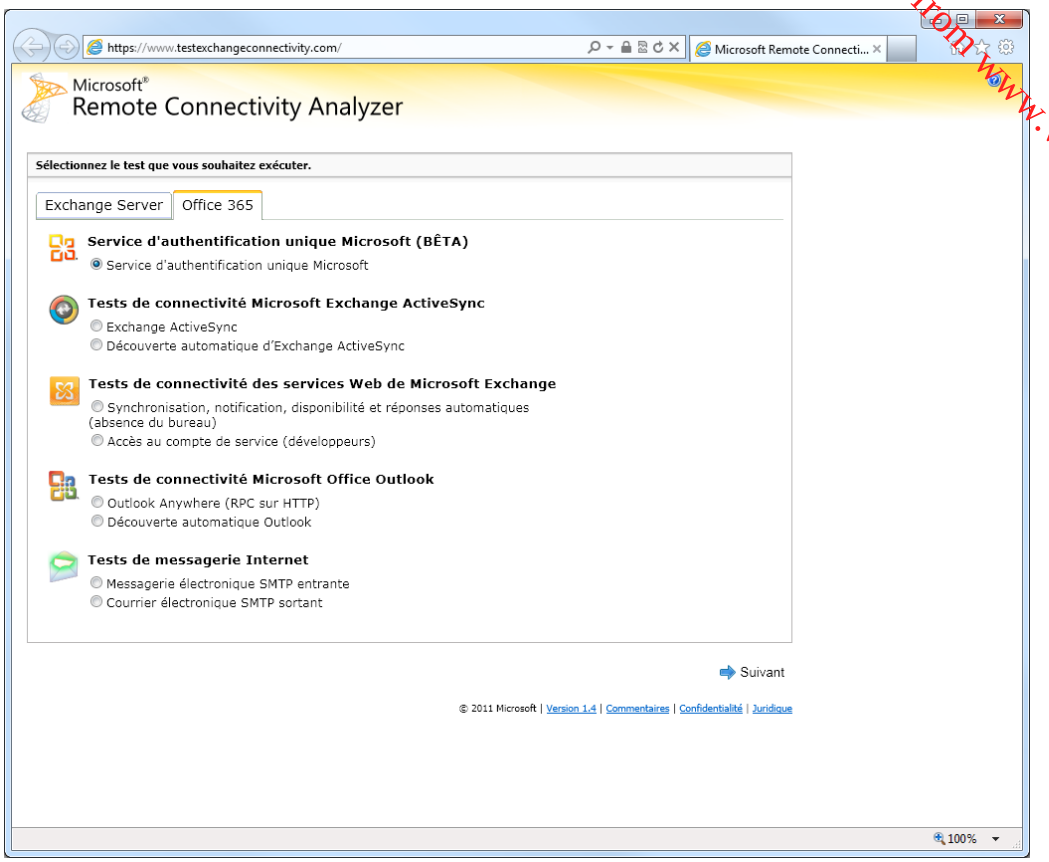


L'outil Microsoft Remote Connectivity Analyzer (RCA)[94] peut également être utilisé pour diagnostiquer les problèmes d'authentification unique passive Office 365.

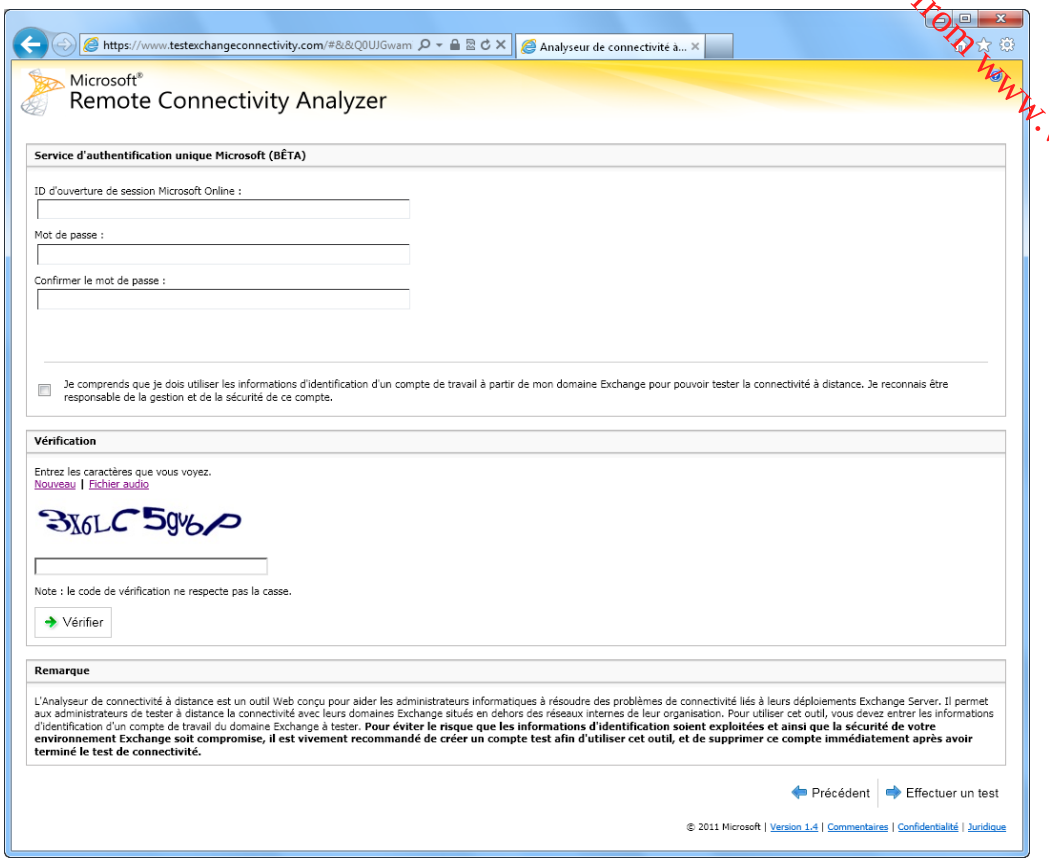
- Pour exécuter RCA pour tester l'authentification unique, procédez ainsi :

1. Ouvrez un navigateur web, et accédez à https://testexchangeconnectivity.com.
2. Cliquez sur l'onglet **Office 365**.

[94] Microsoft Remote Connectivity Analyzer (RCA): https://www.testexchangeconnectivity.com/



3. Sélectionnez **Service d'authentification unique Microsoft**, puis cliquez sur **Suivant**.



4. Tapez votre nom UPN d'entreprise local et votre mot de passe, cochez la case d'avertissement de sécurité, tapez le code de vérification, puis cliquez sur **Effectuer un test**.

Le guide de dépannage AD FS 2.0 (éventuellement en anglais)[95] peut être également utilisé pour résoudre les problèmes.

5.2 Présentation du flux d'authentification profil passif/web

Dans le schéma ci-dessous, l'utilisateur essaie d'accéder à un service web Office 365 tel que SharePoint Online ou Outlook Web Apps (OWA) à partir d'un navigateur sur un ordinateur de travail joint au domaine connecté au réseau d'entreprise.

Lors de l'authentification sur Office 365, les navigateurs Internet établissent une connexion au service de fédération AD FS 2.0 de l'organisation, pour demander un jeton de connexion SAML 1.1.

L'authentification sur le service de fédération AD FS a lieu à l'aide de l'authentification Windows intégrée (Kerberos ou NTLMv2), et ne nécessite pas d'interaction avec l'utilisateur ou d'invite. Le jeton de connexion est présenté au service de connexion Office 365, accordant l'accès au service Office 365.

[95] GUIDE DE DEPANNAGE AD FS 2.0 : http://technet.microsoft.com/en-us/library/adfs2-troubleshooting-guide(WS.10).aspx

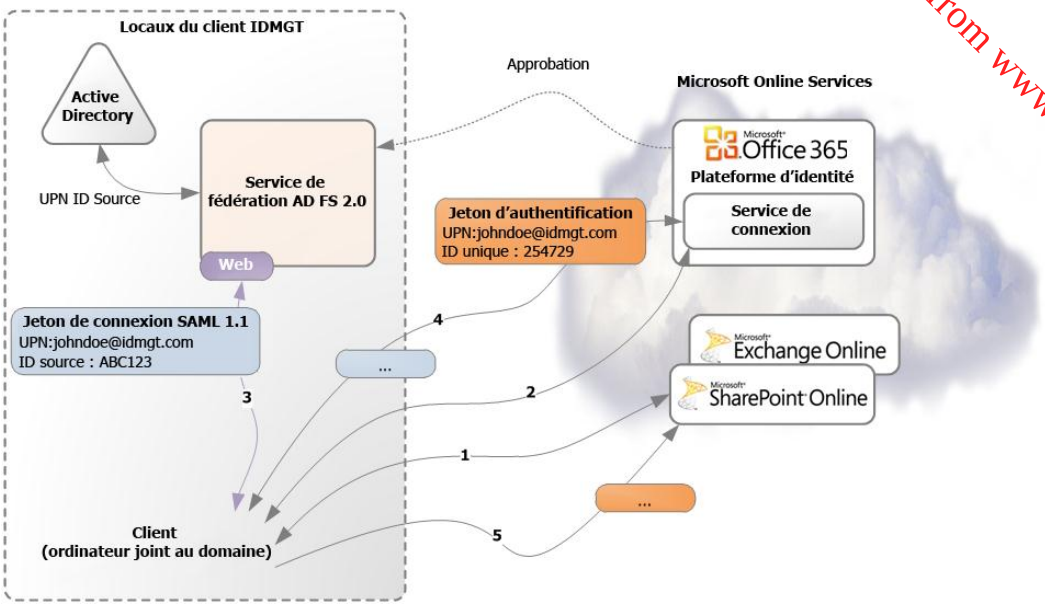


Figure 8Flux d'authentification profil passif/web

Le flux d'authentification profil passif est le suivant :

1. L'utilisateur accède au service web Office 365. Le service indique au client qu'il a besoin d'un jeton d'authentification signé par le service de connexion Office 365, et retourne l'URL du service de connexion de la plateforme des identités Office 365 via une requête HTTP 302 redirigée afin d'obtenir un ticket.
2. Le client demande un jeton d'authentification au service de connexion Office 365. Le service de connexion lit le nom UPN tapé par l'utilisateur et l'identifie comme domaine fédéré. Il indique ensuite que la connexion est impossible, car il a besoin d'un jeton de connexion signé par votre fournisseur de revendications local, c'est-à-dire le service de fédération AD FS 2.0 local. Il retourne donc l'URL du point de terminaison passif du service de fédération AD FS 2.0 (*adfs/ls/*) via une requête HTTP 302 redirigée.
3. Le client demande un jeton de connexion au service de fédération AD FS 2.0. Le service de fédération AD FS 2.0 demande à l'utilisateur de s'authentifier (via l'authentification Windows intégrée par défaut dans cette configuration) sur l'Active Directory local, et si l'authentification réussit, interroge l'Active Directory local pour extraire les revendications utilisateur, puis émet un jeton SAML 1.1 contenant les revendications de l'utilisateur connecté c'est-à-dire ses UPN et Source ID (ImmutableID), qu'il signe à l'aide du certificat de signature de jeton X.509 actuellement déclaré.
4. Le client présente via HTTP POST le jeton SAML 1.1 signé au service de connexion Office 365. Le service de connexion vérifie que le jeton entrant est signé par le fournisseur de revendications approuvé pour le domaine fédéré via la clé publique du certificat de signature X.509 qui a été partagé lors de l'établissement de l'approbation via les métadonnées exposées. Il transforme le Source ID en identificateur unique interne (Unique ID) à partir de la plateforme des identités Office 365, puis émet un nouveau jeton avec UPN et Unique ID, qu'il signe. Cela crée le jeton d'authentification.
5. Le jeton d'authentification retourne vers le client et ce dernier le présente au service de la partie de confiance web Office 365. Le service de la partie de confiance ouvre le jeton, vérifie qu'il est signé par le fournisseur de revendications approuvé (la plateforme des identités Office 365), sur la base d'une clé publique partagée. Il examine la revendication Unique ID et recherche un utilisateur dans son annuaire avec cet Unique ID. (Unique ID est défini dans le cadre de la configuration/création de l'utilisateur et synchronisé avec le service.) Une fois

l'utilisateur trouvé, le service peut appliquer les vérifications de contrôle d'accès nécessaires avant d'autoriser l'utilisateur à accéder au service web Office 365 demandé.

Ce processus semble assez compliqué, mais quand il est décomposé ainsi, cela vous permet de comprendre comment il fonctionne. Si une erreur se produit, il est assez facile de déterminer à quel endroit il faut commencer à résoudre le problème.

Pour plus d'informations, voir l'article Fonctionnement de l'authentification unique dans Office 365 (éventuellement en anglais)[96]. Pour le protocole, voir le chapitre n° 13 WEB (PASSIVE) REQUESTORS de la norme OASIS WS-Federation (WS-Fed) (éventuellement en anglais)[97]. Si vous souhaitez capturer le flux, vous pouvez utiliser une application de suivi réseau ou l'outil Fiddler (avec Fiddler Inspector for Federation Messages (éventuellement en anglais)[98]. Pour ce dernier, voir l'article AD FS 2.0 : Comment utiliser Fiddler Web Debugger pour analyser une connexion passive WS-Federation (éventuellement en anglais)[99].

5.3 Présentation du flux d'authentification profil MEX/client riche

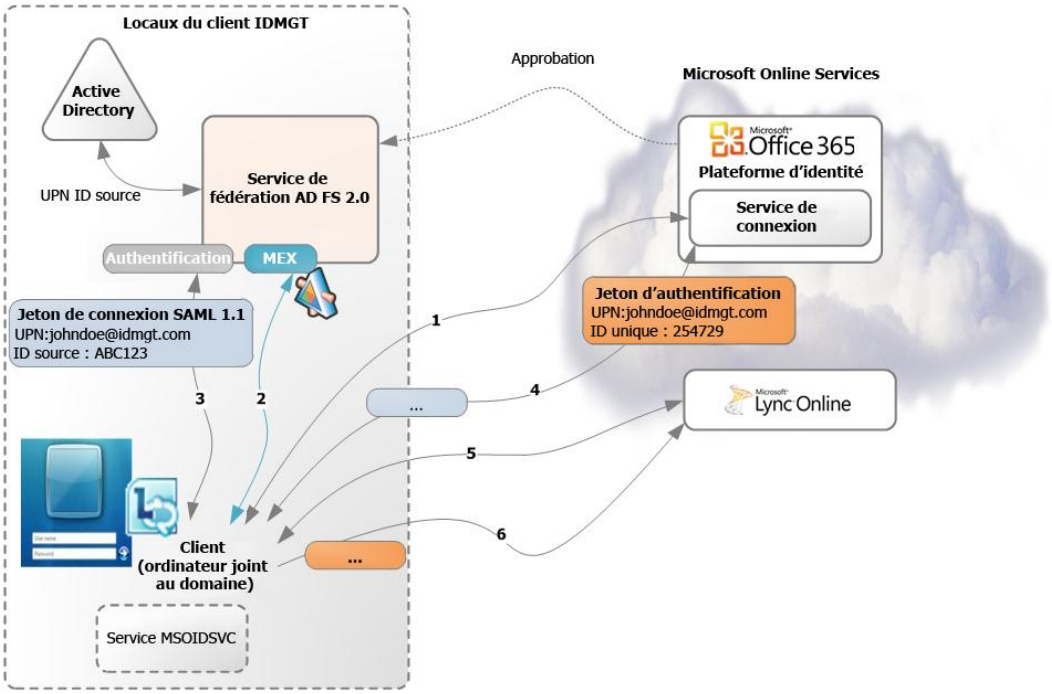


Figure 9Flux d'authentification profil MEX/client riche

Dans le schéma ci-dessus, l'utilisateur essaie d'accéder à Lync Online à partir d'un ordinateur de bureau joint au domaine. Le flux d'authentification profil actif est le suivant :

---

[96] FONCTIONNEMENT DE L'AUTHENTIFICATION UNIQUE DANS OFFICE 365 : http://community.office365.com/en-us/w/sso/727.aspx

[97] WEB SERVICES FEDERATION LANGUAGE (WS-FEDERATION) VERSION 1.2 : http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf

[98] Fiddler Inspector for Federation Messages : http://social.technet.microsoft.com/wiki/contents/articles/fiddler-inspector-for-federation-messages.aspx

[99] AD FS 2.0 : COMMENT UTILISER FIDDLER WEB DEBUGGER POUR ANALYSER UNE CONNEXION PASSIVE WS-FEDERATION : http://social.technet.microsoft.com/wiki/contents/articles/3286.aspx

1. L'utilisateur ouvre une session sur l'ordinateur de travail joint au domaine sur le réseau d'entreprise. Après s'être connecté, le service MSOIDSVC client, c'est-à-dire le service Assistant de connexion Microsoft Online Services (MOS SIA) (voir section n° 3.1.2 Éléments requis pour les ordinateurs de travail) s'ouvre et obtient le domaine Active Directory de l'utilisateur connecté en regardant le suffixe du domaine de son nom UPN. Le service MSOIDSVC appelle un service HRD (home realm discovery) sur le service de connexion de la plateforme des identités Office 365.

   Le service de connexion vérifie si le domaine est un domaine fédéré enregistré. Si tel n'est pas le cas, il ne retourne rien. Si c'est le cas, le service de connexion retourne l'URL du point de terminaison d'échange de métadonnées (point de terminaison MEX) du serveur de fédération enregistré, c'est-à-dire le service de fédération AD FS 2.0 local de l'organisation.

2. Si rien n'est retourné, le service MSOIDSVC a terminé. Si une URL du point de terminaison MEX est retournée, le service MSOIDSVC contacte le point de terminaison MEX (*/adfs/services/trust/mex/*) du service de fédération, qui retourne une liste des points de terminaison WS-Trust exposés par le service de fédération.

3. Le service MSOIDSVC choisit le type de point de terminaison d'authentification approprié (pour l'authentification Windows intégrée (Kerberos ou NTLMv2)) afin de demander un jeton de connexion SAML 1.1. À partir du point de terminaison d'authentification choisi, il procède à l'authentification via Kerberos ou NTLMv2. Une fois authentifié, le service de fédération obtient le jeton NTLMv2 ou le ticket Kerberos de l'utilisateur connecté, interroge l'Active Directory local pour extraire les revendications utilisateur, puis émet un jeton de connexion SAML 1.1 contenant les revendications de l'utilisateur connecté (UPN et Source ID (ImmutableID)), qu'il signe avec le certificat de signature de jeton X.509 actuellement déclaré. Le jeton de connexion est retourné au service MSOIDSVC.

4. Le service MSOIDSVC demande un jeton d'authentification au service de connexion Office 365, en fournissant le jeton de connexion SAML 1.1 reçu du service de fédération AD FS 2.0.

   Le service de connexion Office 365 vérifie le jeton de connexion entrant, transforme Source ID en identificateur unique interne (Unique ID) à partir de la plateforme des identités Office 365, puis émet un nouveau jeton d'authentification (contenant les revendications UPN et Unique ID), qu'il renvoie au client. Ce jeton d'authentification peut être utilisé pour la connexion. Cette procédure s'exécute de façon transparente pour l'utilisateur au moment de la connexion.

   Le service MSOIDSVC met en cache ce jeton qui est prêt à être utilisé par les applications clientes.

5. L'utilisateur démarre Lync 2010. Lync 2010 essaie de se connecter à Lync Online, et demande un jeton d'authentification.

6. Lync 2010 (via un appel in-process à *MSOIDCLI.dll*) demande un ticket d'authentification au service MSOIDSVC. Ce service en a déjà un et l'envoie à Lync Online. Lync Online traite le jeton et applique les vérifications de contrôle d'accès nécessaires avant d'autoriser l'utilisateur à accéder au service.

5.4 Présentation du flux d'authentification profil authentification de base/active EAS

Dans le schéma ci-dessous, l'utilisateur ouvre Outlook à partir de son ordinateur de travail joint au domaine. Lors de l'authentification sur Exchange Online, Outlook utilise les informations d'identification Authentification de base sur Office 365, dans une forme chiffrée. La plateforme Office 365 établit à son tour une connexion au service de fédération AD FS 2.0 de l'organisation pour demander un jeton de connexion SAML, en accordant l'accès de l'utilisateur au service Office 365.

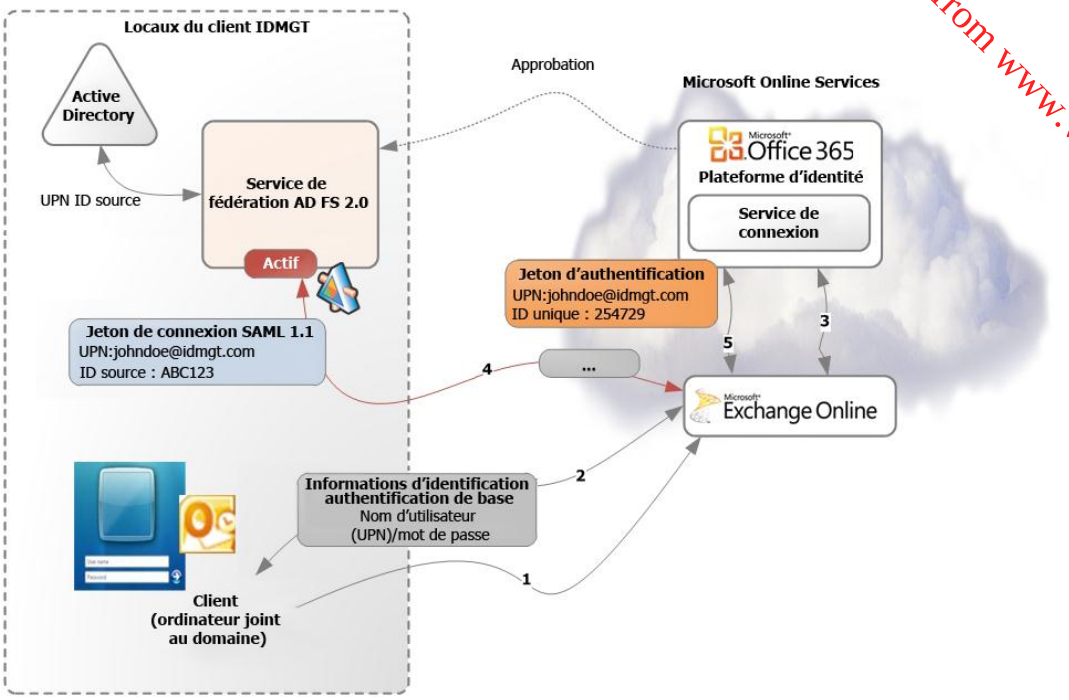


Figure 10Flux d'authentification profil authentification de base/active EAS

Le flux d'authentification profil authentification de base/Active Exchange ActiveSync (EAS) est le suivant :

1. L'utilisateur ouvre une session sur son ordinateur de travail joint au domaine sur le réseau d'entreprise (et le service MSOIDSVC fait l'aller-retour pour obtenir le jeton d'authentification SAML 1.1 et le met en cache). L'utilisateur démarre Outlook 2010.

   Outlook essaie de se connecter à Exchange Online (via l'authentification Windows intégrée et la couche SSPI utilisant Negotiate), mais Exchange Online demande l'authentification de base.

2. Une invite s'affiche à l'utilisateur la première fois et il doit taper ses informations d'identification d'entreprise (son nom d'utilisateur au format UPN et son mot de passe). L'utilisateur peut les enregistrer et il n'aura à les fournir qu'après un changement de mot de passe. Ces données sont envoyées par Outlook à Exchange Online.

3. Exchange Online procède à une action appelée « Proxy Auth », c'est-à-dire qu'il crée une représentation fantôme de l'utilisateur. Il envoie ensuite le domaine/nom UPN de l'authentification de base au service de connexion Office 365.

   La plateforme des identités Office 365 retourne l'URL du point de terminaison profil actif (*/adfs/services/trust/2005/usernamemixed*) du service de fédération AD FS 2.0 local de l'organisation.

4. Exchange Online envoie les informations d'identification de l'authentification de base au point de terminaison du profil actif du service de fédération.

   Le service de fédération authentifie l'utilisateur avec les informations d'identification de base sur l'Active Directory local, interroge l'Active Directory local pour extraire les revendications utilisateur, puis émet un jeton de connexion SAML 1.1 (contenant les revendications UPN et Source ID (ImmutableID) de l'utilisateur), qu'il signe avec le certificat de signature de jeton X.509 actuellement déclaré. Ce jeton est retourné à Exchange Online.

5. Exchange Online l'envoie au service de connexion Office 365. Le service de connexion vérifie le jeton de connexion et le convertit en jeton d'authentification, qui contient UPN et

l'identificateur unique interne (Unique ID) de la plateforme des identités Office 365). Ce jeton d'authentification peut être utilisé pour la connexion.

Exchange Online peut désormais authentifier l'utilisateur avec le jeton d'authentification et supprime la représentation fantôme de l'utilisateur.

Il est à noter que les informations d'identification du client ne sont pas persistantes dans ce processus d'authentification et que les informations d'identification du client ne sont pas stockées ou mises en cache dans les centres de données Microsoft.

De plus, comme indiqué ci-dessous, afin de ne pas avoir à entrer les informations d'identification à chaque session Outlook, les utilisateurs peuvent choisir de mettre en cache leurs informations d'identification dans le gestionnaire d'informations d'identification Windows, en sélectionnant l'option **Enregistrer le mot de passe** à l'invite Outlook.

Le gestionnaire d'informations d'identification Windows fournit une zone sécurisée pour stocker les informations d'identification utilisateur, ce qui permet un accès plus facile aux services distants. Les mots de passe stockés peuvent être protégés à plusieurs niveaux :

- pour les ordinateurs joints au domaine, le mot de passe utilisateur doit être connu pour accéder au contenu du gestionnaire d'informations d'identification ;
- pour contrecarrer les vols de disque dur, le déploiement de technologies de chiffrage de disque peut être utile, par exemple Bit locker sur Windows 7 ;
- les stations de travail personnelles et autres clients non gérés peuvent poser un risque si les mots de passe sont mis en cache localement. Les clients peuvent implémenter des stratégies d'accès client (voir section n° 6.3.2 Utilisation de la stratégie d'accès du client) pour empêcher la connexion à leurs services Office 365 en dehors de leur réseau, ce qui limite les risques de mise en cache des mots de passe par les employés sur des clients non gérés.

6 Autres informations à prendre en compte

Cette section fournit des informations que vous devez connaître liées à l'authentification unique. Vous pouvez également consulter l'article Configuration des options avancées pour AD FS 2.0 et Office 365 (éventuellement en anglais)[100].

6.1 Prise en charge de plusieurs domaines de premier niveau

Jusqu'à la parution du correctif cumulatif 1 pour AD FS 2.0, les organisations qui utilisaient la fonctionnalité d'authentification unique via AD FS 2.0 et qui avaient plusieurs domaines de premier niveau pour les suffixes UPN de l'utilisateur au sein de leur organisation (par exemple, @idmgt.fr ou @idmgt.co.uk) devaient déployer une instance séparée du service de fédération AD FS 2.0 pour chaque suffixe.

Après l'installation du correctif cumulatif 2 (ou du précédent correctif cumulatif 1) sur tous les serveurs de fédération AD FS 2.0 et après avoir suivi les instructions d'utilisation de cette fonctionnalité avec Office 365, les nouvelles règles de revendication sont définies pour générer dynamiquement les ID d'émetteur de jeton basés sur les suffixes UPN des utilisateurs.

Il en résulte que, vous n'avez pas à configurer plusieurs instances du service de fédération AD FS 2.0 pour prendre en charge l'authentification unique pour plusieurs domaines de premier niveau (sans sous-domaines) dans Office 365. Cela nécessite l'utilisation du nouveau commutateur **SupportMultipleDomain** avec le module Microsoft Online Services pour Windows PowerShell.

> **Remarque importante :**
>
> *Ce commutateur n'est pas requis quand vous utilisez un domaine de premier niveau avec plusieurs sous-domaines. Par exemple, si les domaines utilisés pour les suffixes UPN sont @legal.idmgt.fr, @paris.idmgt.fr et @idmgt.fr et que le domaine de premier niveau (idmgt.fr dans ce cas) a été ajouté en premier et fédéré, vous n'avez pas besoin d'utiliser le commutateur **SupportMultipleDomain**. En effet, les sous-domaines sont gérés au sein de l'étendue du parent et un service de fédération unique AD FS 2.0 peut être utilisé pour gérer cela.*

Si vous avez plusieurs domaines de premier niveau (@idmgt.fr et @ idmgt.co.uk) et que ces domaines ont des sous-domaines (@paris.idmgt.fr et @london.idmgt.co.uk), le commutateur **SupportMultipleDomain** ne fonctionnera pas pour les sous-domaines et ces utilisateurs ne seront pas en mesure de se connecter. Ce problème est lié au fait que l'URI émetteur dans le jeton de connexion émis par le service de fédération AD FS 2.0 est utilisé pour rechercher l'espace de noms dans le service de connexion Office 365.

Une approche possible consiste à configurer une expression régulière dans les règles de transformation d'émission de l'approbation de la partie de confiance de la **plateforme des identités Office 365** (voir section n° 5.1.4.2 Règles de transformation d'émission) pour tronquer le nom de domaine de l'URI émetteur :

```
c:[Type == "http://schemas.xmlsoap.org/claims/UPN"]
 => issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/issuerid",
    Value = regexreplace(c.Value, ".+@(?<domain>.+)", "http://${domain}/adfs/services/trust/"));
```

[100] CONFIGURATION DES OPTIONS AVANCEES POUR AD FS 2.0 ET OFFICE 365 : http://technet.microsoft.com/fr-fr/library/hh237448(WS.10).aspx

Des informations supplémentaires sont fournies dans l'article Support pour plusieurs domaines de premier niveau (éventuellement en anglais)[101].

6.2 Prise en charge de l'authentification forte (2FA) pour Office 365

Le service de fédération AD FS 2.0, c'est-à-dire une batterie de serveurs de fédération AD FS 2.0 (voir section n° 4.2.1.1 Scénario 1 - AD FS 2.0 totalement implémenté), réside dans le réseau d'entreprise et authentifie les utilisateurs d'entreprise sur le réseau interne en utilisant par défaut l'authentification Windows intégrée (IWA).

Cependant, il est fréquent que les utilisateurs d'entreprise doivent accéder à leurs ressources habituelles, telles que des services dans Office 365 qui résident sur le nuage, quand ils se trouvent à distance, chez eux, à l'aéroport, dans un café Internet, etc.

Afin de bénéficier des fonctionnalités d'authentification unique présentées dans ce document, les utilisateurs doivent pouvoir accéder au service de fédération AD FS 2.0 afin de pouvoir demander des jetons d'authentification pour accéder aux services si nécessaire.

Dans ces cas précis et pour que les utilisateurs puissent accéder à distance au service de fédération AD FS 2.0, les organisations utilisent le réseau de périmètre comme serveur edge de contrôle d'accès via le serveur proxy de fédération AD FS 2.0, un mode de déploiement d'AD FS 2.0 conçu spécialement pour fournir un accès distant au service de fédération AD FS 2.0 hébergé en interne, et autoriser l'accès via proxy aux services dans Office 365.

> **Remarque :**
>
> *D'autres proxys peuvent être utilisés pour exposer le service de fédération AD FS 2.0 en dehors du réseau d'entreprise comme décrit dans la section n° 2.4.4.2 AUTRES PROXYS. La suite de cette section s'intéresse au serveur proxy de fédération AD FS 2.0.*

Il est géré dans l'infrastructure de l'organisation (localement) et ne nécessite aucune précaution particulière.

Les organisations qui autorisent l'accès distant considèrent que les techniques d'authentification forte sécurisent l'accès entrant. Dans la mesure où les personnes malveillantes peuvent atteindre facilement le point d'accès entrant, et qu'une authentification réussie sur une batterie de serveurs de fédération donne accès aux jetons de sécurité de nombreuses parties de confiance, la sécurisation de l'authentification distante est très importante.

L'authentification forte ou à deux facteurs (2FA) fournit une sécurité améliorée, car elle exige que l'utilisateur réponde à deux critères d'authentification, par exemple « quelque chose de connu » (un nom d'utilisateur/mot de passe) associé à « *quelque chose que vous avez* » (un jeton ou un certificat).

L'activation de l'authentification forte pour les clients web en dehors du réseau de l'organisation est prise en charge avec Office 365.

La prise en charge 2FA n'est pas disponible pour les clients autres que les navigateurs web. Outlook 2010, Lync 2010, ActiveSync, et les autres clients riches ne peuvent pas demander aux utilisateurs des informations d'identification d'authentification forte et donc ne sont pas pris en charge.

Cependant, il existe des exceptions à cette règle en raison de la transition à des interactions de navigateur lors de l'authentification. En effet, quand un client Office 2007 Service Pack 2 (SP2) ou

[101] SUPPORT POUR PLUSIEURS DOMAINES DE PREMIER NIVEAU : http://community.office365.com/en-us/w/sso/support-for-multiple-top-level-domains.aspx

Office 2010 (Word, Excel ou PowerPoint) essaie d'accéder à une bibliothèque de documents SharePoint Online, le client attend une réponse de SharePoint Online dans une fenêtre de boîte de dialogue de navigateur qui prend à son tour en charge les protocoles web de fédération (WS-Federation) qui se basent sur les schémas de redirection.

Dans ce scénario, l'authentification forte est obtenue en configurant le serveur proxy de fédération pour exiger l'authentification 2FA pour le point de terminaison « Fédération passive » (voir section n° 5.2 Présentation du flux d'authentification profil passif/web).

> **Remarque importante :**
>
> *l'authentification forte ne doit être appliquée qu'au point de terminaison « fédération passive », car les autres clients ne seraient pas en mesure de se connecter.*

Elle est gérée dans l'infrastructure de l'organisation (localement) et ne nécessite aucune configuration particulière sur Office 365 Online Services. C'est pourquoi, les organisations auront besoin de déployer leur propre infrastructure 2FA (si nécessaire).

La mise en œuvre de l'authentification 2FA avec l'authentification unique pour les utilisateurs qui accèdent aux applications web Office 365 en dehors du réseau d'entreprise est implémentée par l'organisation au niveau du proxy. Cela s'applique également aux clients Office 2007 Service Pack 2 (SP2) ou Office 2010 (Word, Excel ou PowerPoint). Cependant, comme déjà indiqué, les autres applications clientes riches pour Office 365 (Outlook, Lync, etc.) ne sont pas prises en charge.

En ce qui concerne le proxy du serveur de fédération AD FS 2.0, les méthodes de connexion suivantes sont disponibles pour collecter et traiter les informations d'identification 2FA en fonction des fonctionnalités prises en charge du fournisseur de solutions 2FA (tiers) utilisé :

- connexion par carte à puce avec AD FS 2.0 ;
- connexion basée sur les formulaires avec un module IIS HTTP de fournisseur de solutions 2FA tiers ;
- connexion basée sur les formulaires avec une page de connexion AD FS 2.0 personnalisée pour interagir avec le fournisseur de solutions 2FA.

Quand un serveur proxy de fédération (ou un serveur de fédération AD FS 2.0) est installé, une application web ASP.NET, appelée Pages de connexion, est déployée sur le même serveur pour gérer les demandes de fédération passives.

L'application web Pages de connexion s'exécute dans IIS (Internet Information Services), et les pages associées sont situées dans *%SystemRoot%\Inetpub\adfs\ls* et déployées sous le répertoire virtuel */adfs/ls* du site web par défaut dans IIS.

Les pages de connexion gèrent le protocole WS-Federation et exposent les points d'extension qui permettent les personnalisations, et tout particulièrement la personnalisation du comportement de l'authentification basée sur les formulaires (FBA).

> **Remarque :**
>
> *Pour plus d'informations sur la personnalisation des pages de connexion AD FS 2.0, voir la page Vue d'ensemble de la personnalisation des pages de connexion AD FS 2.0 (éventuellement en anglais)*[102] *dans la documentation du SDK d'AD FS 2.0.*

[102] VUE D'ENSEMBLE DE LA PERSONNALISATION DES PAGES DE CONNEXION AD FS 2.0 : http://msdn.microsoft.com/en-us/library/ee895356.aspx

6.2.1 Connexion par carte à puce avec AD FS 2.0

Cette méthode comporte une prise en charge intégrée pour l'authentification basée sur une carte à puce. Lors de l'utilisation de cartes à puce, le service de fédération AD FS 2.0 peut envoyer une revendication d'authentification forte aux applications et services en aval qui peuvent effectuer des autorisations en fonction de la force de l'authentification.

6.2.2 Connexion basée sur les formulaires avec un module IIS HTTP de fournisseur de solutions 2FA tiers

Cette méthode suppose que le fournisseur de solutions 2FA tiers prend en charge un module Internet Information Services (IIS) HTTP compatible avec la version d'IIS utilisée dans Windows Server 2008 ou Windows Server 2008 R2 et installée sur chaque serveur proxy de fédération AD FS 2.0 de votre organisation. Une fois le module installé et configuré sur les proxys, il intercepte le trafic destiné à l'URL du proxy.

Bien que cette méthode ne demande pas de personnalisation basée sur les formulaires et soit facile à configurer, l'expérience de l'utilisateur final n'est pas optimale, car plusieurs redirections ont lieu et l'utilisateur doit fournir au moins deux fois ses informations d'identification, comme indiqué ci-dessous pour le processus d'authentification 2FA :

1. avant de laisser passer le trafic intercepté, le module redirige le navigateur vers la solution 2FA où l'utilisateur final fournit ses informations d'identification 2FA qui sont validées par le service 2FA ;
2. une fois l'authentification réussie sur la solution 2FA, le module autorise le passage du trafic pour qu'il soit géré par le serveur proxy de fédération AD FS 2.0 en redirigeant le navigateur vers la page de connexion du serveur proxy de fédération ;
3. sur cette page, l'utilisateur final fournit ses informations d'identification Active Directory d'entreprise avant d'être authentifié sur l'application web Office 365.

L'article Guide étape par étape AD FS 2.0 : intégration avec RSA SecurID sur l'extranet (éventuellement en anglais)[103] décrit cette méthode avec RSA Authentication Agent 7.0 pour le web pour les jetons IIS[104] et RSA SecurID.

Cette méthode ne demande pas de personnalisation et est facile à mettre en place. Son inconvénient réside dans le fait que l'utilisateur subit plusieurs redirections et doit fournir ses informations d'identification à 2 reprises.

6.2.3 Connexion basée sur les formulaires avec une page de connexion AD FS 2.0 personnalisée

Cette méthode suppose que le fournisseur de solutions 2FA tiers prend en charge une interface qui peut être appelée par du code qui s'exécute en arrière-plan de la page de connexion basée sur les formulaires personnalisée des proxys de serveur de fédération. La page de connexion basée sur les formulaires personnalisée propose des champs supplémentaires à l'utilisateur permettant d'entrer des facteurs d'authentification supplémentaires ou une logique supplémentaire pour les collecter de façon transparente.

Comme indiqué dans l'illustration, vous pouvez utiliser la technologie Login People Digital DNA, et permettre aux utilisateurs d'utiliser l'authentification forte basée sur « *ce qu'ils connaissent* » (un mot

[103] GUIDE ETAPE PAR ETAPE AD FS 2.0 : INTEGRATION AVEC RSA SECURID SUR L'EXTRANET : http://technet.microsoft.com/fr-fr/library/hh344805(WS.10).aspx

[104] RSA Authentication Agent 7.0 pour le web pour IIS : http://www.rsa.com/node.aspx?id=3663

de passe) et sur « *ce dont ils disposent* » (leur ordinateur, smartphone, et/ou clé USB), et créer ainsi un second facteur d'authentification, afin d'obtenir un niveau de sécurité supérieur pour protéger les identités et la confidentialité tout en tirant pleinement parti du potentiel d'interopérabilité d'AD FS 2.0. L'intégration avec ce fournisseur de solutions 2FA tiers est décrite dans le livre blanc Intégration de Login People Digital DNA Server avec AD FS 2.0 pour l'authentification unique fédérée interopérable (éventuellement en anglais)[105].

Bien que cette méthode permette une meilleure expérience pour l'utilisateur (une seule page de connexion basée sur les formulaires est utilisée pour les informations d'identification 2FA et Active Directory) que la méthode décrite ci-dessus, elle demande plus d'efforts d'administration, car il est nécessaire de personnaliser la page de connexion basée sur les formulaires sur chaque serveur proxy de fédération de votre organisation afin de collecter les informations d'identification 2FA et les informations d'identification Active Directory d'entreprise.

6.3 Limitation de l'accès aux services Office 365 en fonction de l'emplacement du client

Vous voudrez contrôler les services dans Office 365 qui sont publiés sur Internet et donc bloquer certains scénarios d'accès externes.

6.3.1 Utilisation de points de terminaison AD FS 2.0

L'accès client au service peut être contrôlé via la publication de points de terminaison AD FS 2.0 (voir section n° 5.1.5 POINTS DE TERMINAISON).

Par exemple, en ne publiant pas le point d'accès Fédération passive, une organisation peut empêcher la connexion des clients web au service en dehors de leur réseau d'entreprise.

> **Remarque importante :**
>
> *Comme indiqué précédemment, pour autoriser les clients Authentification de base à se connecter (y compris Outlook 2010), un serveur proxy de fédération AD FS 2.0 doit être déployé dans tous les cas. Si un serveur proxy de fédération n'est pas disponible, aucun client Outlook 2010 ne pourra s'authentifier, même à partir du réseau d'entreprise interne.*

6.3.2 Utilisation de la stratégie d'accès du client

Prise en charge avec Office 365 depuis octobre 2011, la stratégie d'accès du client, qui nécessite le correctif cumulatif 2 pour AD FS 2.0 (ou le correctif cumulatif 1 précédent pour AD FS 2.0), est fournie pour les services dans Office 365, via une solution tierce :

1. Via les attributs de demande d'authentification qui fournissent les informations sur les clients qui essaient de se connecter. Le serveur proxy de fédération AD FS 2.0 passera cinq nouveaux en-têtes HTTP de contexte de demandes au service de fédération AD FS 2.0 :
   a. *x-ms-forwarded-client-ip*;
   b. *x-ms-client-application*;
   c. *x-ms-client-user-agent*;

[105] INTEGRATION DE LOGIN PEOPLE DIGITAL DNA SERVER AVEC AD FS 2.0 POUR L'AUTHENTIFICATION UNIQUE FEDEREE INTEROPERABLE : http://download.microsoft.com/documents/France/Interop/2011/Integrating-LoginPeople-DDNA-Server.docx

d. *x-ms-proxy*;

e. *x-ms-endpoint-absolute-path*.

> **Remarque importante :**
>
> *Si vous utilisez un serveur proxy tiers, il doit être configuré pour envoyer l'en-tête HTTP x-ms-proxy et inclure la valeur du nom DNS complet de l'hôte proxy, comme indiqué dans le scénario d'implémentation d'AD FS 2.0 par pare-feu (voir section n° 4.2.1.2).*

2. Pour consommer ces informations de contexte de demande supplémentaires, la stratégie d'accès client présente un ensemble de nouveaux types de revendications de contexte de demande :

   a. *http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-forwarded-client-ip*;

   b. *http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-application*;

   c. *http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-user-agent*;

   d. *http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-proxy*;

   e. *http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-endpoint-absolute-path*.

   Sur cette base, une règle de transformation d'acceptation personnalisée pour chaque nouveau type de revendication de contexte de demande doit être ajoutée sur l'approbation du fournisseur de revendications Active Directory (voir section n° 5.1.3 APPROBATION DE FOURNISSEUR DE REVENDICATIONS ACTIVE DIRECTORY LOCAL) afin que les nouveaux types de revendications soient disponibles au moteur de stratégie.

   Par exemple, la règle de revendication pass-through suivante doit être créée pour le type de revendication de contexte de demande *http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-forwarded-client-ip* :

```
c:[Type == "http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-forwarded-client-ip"] =>
issue(claim = c);
```

   D'autres règles de revendications pass-through similaires doivent être créées pour chacun des quatre types de revendications restants.

3. AD FS 2.0 peut alors utiliser les nouvelles revendications de contexte de demande dans le pipeline de revendications et, peut agir en fonction d'elles via les règles personnalisées appropriées définies dans l'ensemble de **règles d'autorisation d'émission** de l'approbation de la partie de confiance de la plateforme des identités Office 365 (voir section n° 5.1.4.3 Règles d'autorisation d'émission).

Le service de fédération AD FS 2.0 peut prendre en charge des stratégies d'accès afin d'autoriser ou d'interdire l'accès en fonction de l'association de la demande d'accès de l'utilisateur, l'adresse IP des appareils et la méthode d'accès, comme indiqué dans l'article Microsoft TechNet Limitation de l'accès à services Office 365 en fonction de l'emplacement du client (éventuellement en anglais)[106].

Une telle solution permet les scénarios suivants :

- **Bloquer l'accès externe à Office 365** : l'accès à Office 365 est autorisé à partir de tous les clients du réseau d'entreprise interne, mais les demandes de clients externes sont refusées en fonction de l'adresse IP du client externe.

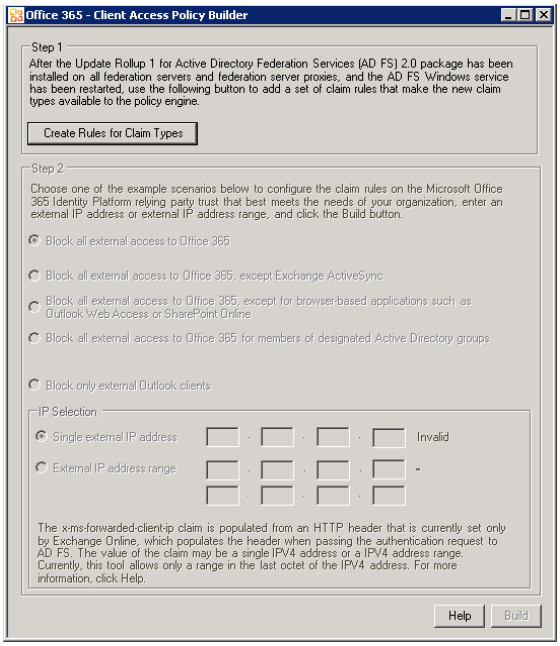
[106] LIMITATION DE L'ACCES AUX SERVICES OFFICE 365 EN FONCTION DE L'EMPLACEMENT DU CLIENT : http://technet.microsoft.com/en-us/library/hh526961(v=ws.10).aspx

- **Bloquer l'accès externe à Office 365, sauf pour Exchange ActiveSync (EAS)** : l'accès à Office 365 est autorisé à partir de tous les clients du réseau d'entreprise interne, ainsi qu'à partir d'appareils clients externes, tels que des smartphones, qui utilisent EAS. Tous les autres clients externes sont bloqués.
- **Bloquer l'accès externe à Office 365, à l'exception des applications de navigateur, telles que SharePoint Online ou Outlook Web App (OWA)** : bloque l'accès externe à Office 365, sauf pour les services web Office 365.
- **Bloquer l'accès externe à Office 365 pour les membres de groupes Active Directory spécifiques** : ce scénario est utilisé pour tester et valider le déploiement de stratégie d'accès client. Il bloque l'accès externe à Office 365 uniquement aux membres d'un ou plusieurs groupes Active Directory. Il peut également être utilisé pour fournir l'accès externe uniquement aux membres d'un groupe.

L'outil Client Access Policy Builder (éventuellement en anglais)[107] permet de configurer ces stratégies d'accès client AD FS 2.0 personnalisées plus facilement et efficacement.

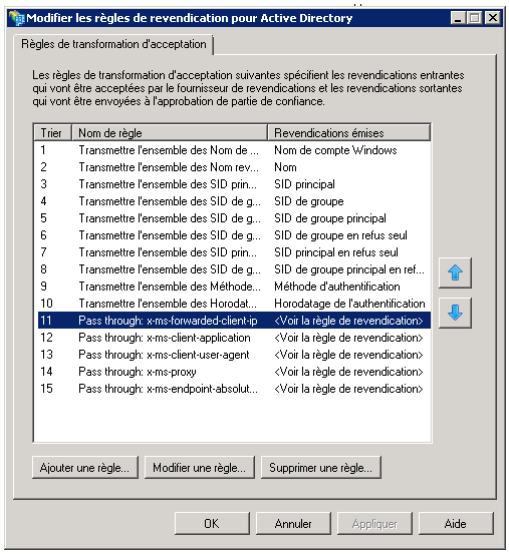
▶ Pour configurer des stratégies d'accès client AD FS 2.0 personnalisées avec cet outil, procédez ainsi :

1. Téléchargez l'outil à partir de la galerie en ligne et enregistrez le fichier *Office_365_-_Client_Access_Policy_Builder.ps1* sur le bureau.
2. Cliquez avec le bouton droit sur le fichier *Office_365_-_Client_Access_Policy_Builder.ps1*, cliquez sur **Propriétés**, sur **Débloquer** sous l'onglet **Général**, puis cliquez sur **OK**.
3. Cliquez avec le bouton droit sur *Office_365_-_Client_Access_Policy_Builder.ps1*, puis cliquez sur **Exécuter avec PowerShell**.



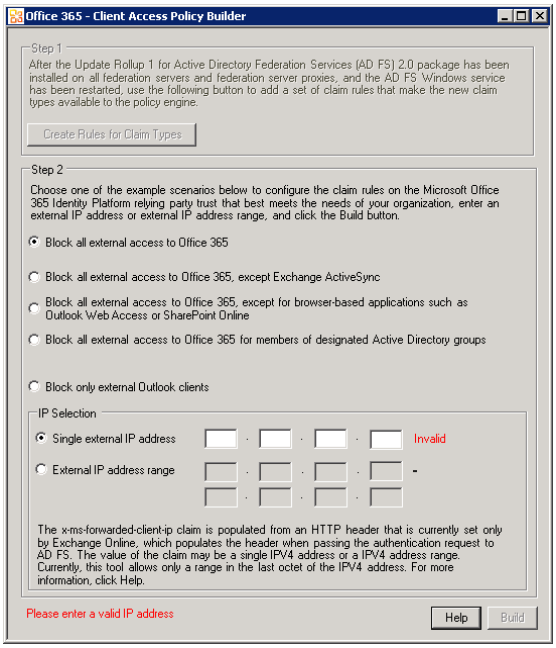
4. Cliquez sur **Create Rules for Claim Types** pour créer les cinq règles de revendication provisoires dans l'approbation du fournisseur de revendications Active Directory.

[107] Outil Client Access Policy Builder : http://gallery.technet.microsoft.com/scriptcenter/Client-Access-Policy-30be8ae2



Si l'outil détecte la présence de règles provisoires de stratégie d'accès client existantes, il ne fera rien, et cela sera indiqué dans l'interface.

5. Une fois l'**Étape 1** de **Office 365 - Client Access Policy Builder** terminée, l'interface déverrouille l'**Étape 2**.



6. Sélectionnez un scénario de stratégie d'accès client dans la liste.
7. Tapez l'adresse IP externe de votre environnement en regard de **Single external IP address**. Si vous utilisez une plage d'adresses IP externes, choisissez **External IP address range** et indiquez la plage dans l'outil **Office 365 - Client Access Policy Builder**.
8. Une fois le scénario sélectionné et une adresse IP externe valide entrée, cliquez sur le bouton **Build** pour générer les règles de revendications pour votre approbation de partie de confiance de la plateforme des identités Office 365 .

6.4 Utilisation de liaisons intelligentes pour Office 365

Les liaisons intelligentes pour Office facilitent l'accès aux charges de travail Office 365 avec des identités fédérées. Les liaisons intelligentes sont des liens déjà mis en forme qui fonctionnent avec les charges de travail web passives suivantes , Microsoft Online Portal (MOP), Outlook Web Access (OWA), et SharePoint Online (SPO).

L'utilisation de liens déjà mis en forme simplifie le processus de connexion des utilisateurs fédérés. Quand un utilisateur s'authentifie sur ces charges de travail Office 365, le comportement par défaut consiste à demander à l'utilisateur d'entrer son UPN à l'invite login.microsoftonline.com pour déclencher le processus HRD (home realm discovery) avant qu'il soit redirigé vers le service de fédération AD FS 2.0 local (voir section n° 4.4 Vérification de l'authentification unique).

Si vous préférez une expérience de connexion totalement transparente à partir des ordinateurs de travail joints au domaine, vous pouvez déployer et utiliser des liaisons intelligentes personnalisées pour ignorer l'invite HRD.

L'article Utilisation de liaisons intelligentes ou de l'authentification initiée par IdP avec Office 365 (éventuellement en anglais)[108] décrit comment personnaliser les liaisons intelligentes en fonction de vos services Office 365.

- Pour vous connecter à Microsoft Online Portal (MOP), vous pouvez utiliser les liaisons intelligentes suivantes :

https://adfs.demo.idmgt.archims.fr/adfs/ls/?wa=wsignin1.0&wtrealm=urn:federation:MicrosoftOnline (éventuellement en anglais)

- ou -

https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=demo.idmgt.archims.fr&wreply=https:%2f%2fportal.microsoftonline.com%2fdefault.aspx

- Pour vous connecter à Outlook Web Access (OWA), utilisez les liaisons intelligentes suivantes :

https://outlook.com/owa/o365a@demo.idmgt.archims.fr

- ou -

https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=demo.idmgt.archims.fr&wreply=https:%2f%2foutlook.com%2fowa%2fo365a40demo%2eidmgt%2earchims%2efr%2f?exsvurl=1&ll-cc=en-US

- Pour vous connecter à SharePoint Online (SPO), utilisez les liaisons intelligentes suivantes :

https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=demo.idmgt.archims.fr&wreply=https:%2f%2fidmgt%2esharepoint%2ecom%2f%5fforms%2fdefault%2easpx

Remplacez dans les liens précédents les parties soulignées en jaune par les valeurs appropriées du point de terminaison public de fédération passif du service de fédération AD FS 2.0, du domaine fédéré ou de l'UPN de l'utilisateur qui correspondent à votre configuration.

Les paramètres de chaîne de requête sont détaillés dans la norme OASIS WS-Federation (WS-Fed) (éventuellement en anglais)[109] (voir chapitre n°13 WEB (PASSIVE) REQUESTORS).

---

[108] UTILISATION DE LIAISONS INTELLIGENTES OU D'UNE AUTHENTIFICATION INITIEE PAR IDP AVEC OFFICE 365 : http://community.office365.com/en-us/w/sso/using-smart-links-or-idp-initiated-authentication-with-office-365.aspx

[109] WEB SERVICES FEDERATION LANGUAGE (WS-FEDERATION) VERSION 1.2 : http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf