Microsoft SharePoint Online for Enterprises

Discovery Questionnaire

Author: Ryan Berg

Published: March 2013

Contents

Chapter 1 Customer Information

Customer name: *(Enter your company name here)*

Questionnaire date: *(Enter today's date here)*

Deployment consultant: *(Enter the name of your SharePoint online deployment consultant here)*

Chapter 2 Launch Date

Provide the date of your planned business launch. This is the date you plan to release SharePoint Online to your end users. The launch date may depend on several factors, including rollout of customizations, updating desktops, or other business or technical dependencies.

If you are not planning customizations or content migration, the business launch can be scheduled for the same day as the Customer Validation of Service (CVS). Otherwise, please specify the date when you plan to launch to end users.

Is your business launch at CVS? *(Yes or no)*

If you answered “no,” when is your planned business launch date? *(Enter launch date here)*

Chapter 3 Prerequisites

The following list of prerequisites must be met in order for your deployment to be successful:

- ***Security Assertion Markup Language (SAML) prerequisites:***
  - Your security token service (STS) product (for example, Microsoft Active Directory® Federation Services (AD FS)) must be set up and ready for trust configuration as part of the overall completion of the Microsoft SharePoint Online IT Requirements document.
- ***Partner Access prerequisites:***
  - If you are planning to expose the Partner Access Web App to the Internet, you must ensure the corresponding Domain Name System (DNS) entries are in place to ensure functionality.
  - You must submit the Configuration Request (CR) template Add Internet Access to Web Applications [SPOD-13-130A] in order to have the Partner Access Web App available over the Internet.
  - If you only want the Partner Web App URL available via the Internet, you must specify this in the CR template.

Chapter 4 SharePoint Online Application-Level Configuration

section 4.1
SharePoint Online URLs

Specify what URLs will be used to access the SharePoint Online home page, Team Sites, and SkyDrive Pro sites (formerly called My Sites). Each URL must be in the form of a fully qualified domain name (FQDN); for example: `contoso.sharepoint.net`, `teamcontoso.sharepoint.net`, and `mycontoso.sharepoint.net`.

All three of these Web applications must be provisioned upon release.

Note
Once the Service has been released to the customer, the URLs denoted for Portal, Team Sites, or SkyDrive Pro sites cannot be changed.

Important
Self-service site creation is enabled for all by default.

To specify the URLs for your SharePoint Online site, enter them in the following table.

URL*	FQDN	Internet Accessible?†
Portal URL	*(Enter FQDN for Portal here)*	*(Should users be permitted to access the Portal site securely from the Internet? Yes or no)*
Team Sites URL	*(Enter FQDN for Team Sites here)*	*(Should users be permitted to access Team Sites securely from the Internet? Yes or no)*
SkyDrive Pro URL	*(Enter FQDN for SkyDrive Pro here)*	*(Should users be permitted to access SkyDrive Pro securely from the Internet? Yes or no)*

Will the URLs specified in the previous table be used on-premises prior to the release date? *(Yes or no.)*

* All URLs for your SharePoint Online Web applications will share the FQDN pattern (for example, *<site>*.sharepoint.net or *<site>*.sharepoint.contoso.net). SharePoint Online supports up to four-part URLs. SharePoint Online supports up to four-part URLs.

† SharePoint Online access from the Internet is controlled via Access Control Lists (ACLs).

Note
If you answered “yes,” the SharePoint Online team will work with you to time the DNS cutover to the SharePoint Online virtual IPs (VIPs).

section 4.2
SSL Certificate

Subject alternative name (SAN) certificates enable you to protect multiple host names with a single Secure Sockets Layer (SSL) certificate. To enable SharePoint Online to purchase the necessary SSL certificate on your behalf, provide the following information.

Note
The person you list as approver must be available to be contacted using both email and land line voicemail by the certification agency.

Note
PO Box addresses will not be recognized by SharePoint Online.

Company - legal name, as it appears in Dunn and Bradstreet: *(Enter your company’s legal name here)*
Company - organizational unit: (Enter your organizational unit here)
Company - street address: (Enter your company’s street address here)
Company - city: (Enter your company’s city here)
Company - state or province: (Enter your company’s state or province here)
Company - country code (ISO): (Enter your company’s country code (ISO) here)
Approver - full name: (Enter the approver’s full name here)
Approver - department: (Enter the approver’s department here)
Approver - department street address: (Enter the street address of the approver’s department here)
Approver - department city: (Enter the city of the approver’s department here)
Approver - department state or province: (Enter the state or province of the approver’s department here)
Approver - department country code (ISO): (Enter the country code (ISO) of the approver’s department here)
Approver - corporate email address: (Enter the approver’s corporate email address here)
Approver - corporate phone number (land line): (Enter the approver’s corporate phone number here)

section 4.3
Importing User Profiles from Active Directory Domain Services

SharePoint Online may configure profile synchronization to import initial Active Directory-based users into the SharePoint Online application.

The Active Directory Domain Services (AD DS) directory service must be accessible from the SharePoint farm in order to import profiles. See the Microsoft TechNet article “Plan for profile synchronization (SharePoint Server 2013)” (http://technet.microsoft.com/en-us/library/ff182925(v=office.15).aspx) for more details on profile synchronization.

Note
This process also applies to the Partner Access feature. See Chapter 7, Partner Access, for more details.

section 4.3.1
Active Directory Groups

For new customers, a configuration request (CR) is required to import Active Directory groups. By default, Active Directory groups are excluded from the User Profile Synchronization process. Exceptions are made for customers who plan to use the Group Membership Web Part or audience targeting functionality on site collections. The benefits of excluding Active Directory groups from User Profile Synchronization are:

- The process of importing users completes much more quickly (test cases performed by SharePoint Online have completed in hours as opposed to days).

Note
The efficiency of the user profile import is subject to the performance, size, and complexity of the customer directory.

- The process is more predictable, reducing or eliminating altogether the work involved with reconciling group membership changes.
- Profile property updates that require a full profile import will be reflected much sooner. Customers have greater agility in making these kinds of changes.

Do you intend to import Active Directory groups? *(Yes or no)*

section 4.3.2
Information for Accounts Used to Import User Profiles

For each directory service you plan to import users from, provide the following information in the table that follows this bulleted list.

Note
Information is required for each forest and/or domain. Accounts may be used in more than one forest or domain; an account is required for each forest or domain that does not trust the others. A maximum of eight profile synchronization forests and/or domains are allowed.

- A fully-qualified domain name.
- A network service account.
    - The account must have read access to the following values: display name, mail, group type, manager, msRTCSIP primary user address, distinguished name, object GUID, object SID, proxy addresses, sam account name, and surname.
    - This account ***must*** have Replicate Directory Changes permission in every domain in every forest from which profiles will be imported.

      Refer to the Microsoft Knowledge Base article "How to grant the "Replicating Directory Changes" permission for the Microsoft Metadirectory Services ADMA service account" (http://support.microsoft.com/kb/303972) for two methods of setting the Replicate Directory Changes permission.

Note
SharePoint Online recommends using the ACL editor method.

    - If the NetBIOS name of the AD DS domain you want to import data from is different from the domain name, this account also must have Replicate Directory Changes permissions

on the `cn=configuration` container in AD DS. See the Microsoft TechNet article "Plan for profile synchronization (SharePoint Server 2013)" (http://technet.microsoft.com/en-us/library/ff182925(v=office.15).aspx) or more information.

- If your domain controller is running Windows 2003 or earlier functional level, the account ***must*** be a member of the Pre-Windows 2000 Compatible access built-in group. See the Microsoft Knowledge Base article "How To Add Users to the Pre-Windows 2000 Compatible Access Group in Windows Server 2003" (http://support.microsoft.com/kb/325363) for more information.

- The password for the network service account.

Important
A separate password-protected Excel spreadsheet will be sent by your deployment consultant to provide the needed password information to Microsoft. A meeting will be scheduled by your deployment consultant to provide you with the password to the protected spreadsheet.

Once you have added the account information and password(s) to the SharePoint Network Accounts tab in the spreadsheet, perform the following steps:

1. Create an email using the following alias for Microsoft O365 SharePoint: O365SPOEP@microsoft.com
2. Enter the following in the Subject line: <<Customer Name>>.xlsx
3. Attach the encrypted <<Customer Name>>.xlsx spreadsheet to the email.

Warning
Do not include the spreadsheet's encryption password in this email.

The password must be:

- Non-expiring.
- A minimum of 15 characters.
- A mix of upper- and lower-case letters, digits, and include at least one special character: `@!{}[]`

Important
You cannot use the following special characters: comma (,), semi-colon (;), or double quote ("), as the SharePoint profile importer cannot process these characters.

Domain or Forest?	Domain or Forest FQDN	Expected Profile Count	Account Name	Password
(Enter domain or forest here)	*(Enter domain or forest FQDN here (for example,emea.contoso.com))*	*(Enter number here)*	*(Enter account name here (for example domain\account))*	*(Send by secure email. DO NOT ENTER HERE)*

Domain or Forest?	Domain or Forest FQDN	Expected Profile Count	Account Name	Password
(Enter domain or forest here)	*(Enter domain or forest FQDN here (for example,emea.contoso.com))*	*(Enter number here)*	*(Enter account name here (for example domain\account))*	*(Send by secure email. DO NOT ENTER HERE)*
(Enter domain or forest here)	*(Enter domain or forest FQDN here (for example,emea.contoso.com))*	*(Enter number here)*	*(Enter account name here (for example domain\account))*	*(Send by secure email. DO NOT ENTER HERE)*
<add or delete rows as needed>				

section 4.3.3
Filtering Imported Profiles Using FIM

The SharePoint Online application automatically detects all user object attributes and can then exclude users as needed by filtering the profiles based on specific criteria using FIM.

To filter profiles, you must determine what you want to include and exclude based on several criteria.

> **Note**
> This process also applies to the Partner Access feature. See Chapter 7, Partner Access, for more details.

section 4.3.3.1
FIM Filtering Example

To help understand the user import filtering process, review the following example. To skip this example, go to Section 4.3.3.2, Filter Worksheet and FIM Filter Table.

Contoso wants to import all full-time employees from its Redmond location and exclude users if they are contractor-based staff or interns. Contractor staff all have Username values that start with the letter “A,” and interns have employee IDs that start with the digits “200.” Contoso also wants to skip those groups owned by Jacob.

In order to accomplish all of these data migration goals, Contoso would fill out the customer objective worksheet as follows:

Customer Objective	Include	Exclude
1. Redmond users	Users with Location equal to “Redmond”	
2. Contractor staff		Username values with the first character equal to “A”
3. Interns		Users with the first three digits of employee ID equal to “200”
4. Groups		Groups equal to “Jacob”

Using the objectives listed in the Contoso customer objective worksheet, Contoso would then fill out the FIM filter table as follows:

FIM Filter Category	Filter	Expression (AND/OR)‡	Attribute to filter on§	Operator	Value
Exclusion filter for users	Filter 1	OR	SAMAccountName	Starts With	A
	Filter 2	OR	Location	Does not Equal	Redmond
	Filter 3	OR	Employee ID	Starts With	200
Exclusion filter for groups	Filter 1	OR	Owner	Equals	Jacob

section 4.3.3.2
Filter Worksheet and FIM Filter Table

Use the following worksheet to help you identify your objectives for filtering user accounts before entering them in the FIM filter table that follows.

Customer Objective	Include	Exclude
1. *(Enter objective here)*	*(Include users that equal X)*	***OR** (Exclude users that equal X)*
2. *(Enter objective here)*	*(Include users that equal X)*	***OR** (Exclude users that equal X)*
3. *(Enter objective here)*	*(Include users that equal X)*	***OR** (Exclude users that equal X)*
4. *(Enter objective here)*	*(Include users that equal X)*	***OR** (Exclude users that equal X)*
<add or delete rows as needed>		

‡ SharePoint does not support the use of both AND and OR Boolean operators in the same join. You must choose one or the other unless you are using only one filter.

§ The attribute `objectClass=user` is not displayed in the SharePoint UI, but is applied to the profile synchronization filter by default. You do not need to include this attribute in the FIM filter table.

> ⚠ **Important**
> Do not include the attribute `objectCategory=person`. There is no need to filter out non-user objects as it is done by default.

Enter your user FIM filter objectives in the following table.

FIM Filter Category	Filter	Expression (AND/OR)[**]	Attribute to filter on[††]	Operator	Value
(Enter filter category here)	*(Enter filter number here)*	*(AND/OR)*	*(Enter attribute name here)*	*(Enter operator here (for example, equals))*	*(Enter value to match here)*
(Enter filter category here)	*(Enter filter number here)*	*(AND/OR)*	*(Enter attribute name here)*	*(Enter operator here (for example, equals))*	*(Enter value to match here)*
(Enter filter category here)	*(Enter filter number here)*	*(AND/OR)*	*(Enter attribute name here)*	*(Enter operator here (for example, equals))*	*(Enter value to match here)*
(Enter filter category here)	*(Enter filter number here)*	*(AND/OR)*	*(Enter attribute name here)*	*(Enter operator here (for example, equals))*	*(Enter value to match here)*

How many total records are you expecting the FIM filters to return? *(Enter number of total records here)*

[**] SharePoint does not support the use of both AND and OR Boolean operators in the same join.
[††] The attribute `objectClass=user` is not displayed in the SharePoint UI, but is applied to the profile synchronization filter by default. You do not need to include this attribute in the FIM filter table.

Important
Do not include the attribute `objectCategory=person`. There is no need to filter out non-user objects as it is done by default.

Chapter 5 SharePoint Online Permissions

section 5.1
SharePoint Online Web Application User Policy

Provide at least one FQDN and the associated AD DS security group name(s) to be granted full control of all Web applications in the following table. These values are mandatory across all Web applications (Portal, Team Sites, and SkyDrive Pro) and provide the highest level of administrative control.

AD DS Domain	Security Group
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
<add or delete rows as needed>	

section 5.2
Primary and Backup Administrators

Provide the credentials of the accounts to be used for administrators. These accounts are granted full control of the root site collection, including the ability to grant permissions to other users. To add an account, specify its domain and Username, and then select whether it is to be a primary or backup administrative role.

section 5.2.1
Site Collection Administrators

Enter the domain and Username of a primary and backup site collection administrator in the following table. These values are the mandatory primary and secondary values for Web applications (Portal, Team Sites, and SkyDrive Pro). These values are also used to grant permissions to the App Catalog site.

Site Collection Administrator	Domain\Username or user principal name (UPN)
Primary	*(Enter the domain\Username or UPN)*
Backup	*(Enter the domain\Username or UPN)*

section 5.2.2
Pre-Production Environment Site Collection Administrators

Enter the domain and Username of a primary and backup site collection administrator for the pre-production environment (PPE) in the following table. These values are the mandatory primary and secondary values for Web applications (Portal, Team Sites, and SkyDrive Pro) in the PPE. These values are also used to grant permissions to the App Catalog site.

PPE Site Collection Administrator	Domain\Username or UPN
Primary	*(Enter the domain\Username or UPN)*
Backup	*(Enter the domain\Username or UPN)*

section 5.3
Information Workers and Kiosk Workers

Have you purchased kiosk licenses? *(Yes or no)*

If you answered “no,” skip to Section 5.4, Restrict Use of SkyDrive Pro.
If you answered “yes,” please identify your kiosk and information workers in the tables on the following page.

section 5.3.1
Identify Information Workers

Information workers are permitted to use social networking features such as SkyDrive Pro in SharePoint Online. To identify information workers, specify the AD DS security group names that they belong to in the following table.

AD DS Domain	Security Group
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
<add or delete rows as needed>	

section 5.3.2
Identify Kiosk Workers

Kiosk workers are prevented from creating SkyDrive Pro sites in SharePoint Online.

Further information about kiosk workers will be provided in the upcoming SharePoint Online Service Description, available in April of 2013.

To identify kiosk workers, specify the AD DS security group names that they belong to in the following table.

AD DS Domain	Security Group
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
<add or delete rows as needed>	

section 5.4
Restrict Use of SkyDrive Pro

SkyDrive Pro sites are available to all information worker users by default unless you choose to restrict availability.

Do you plan to restrict the availability of Sky Drive Pro Sites? *(Yes or no)*

If you answered “no,” skip to Chapter 6, SharePoint Online Email.
If you answered “yes,” you must specify the AD DS security group names that identify these users.

To restrict the availability of SkyDrive Pro to a specific set of users, specify one or more security groups to identify these individuals in the following table.

> **Important**
> If you answered “yes,” ensure that site collection administrators in Section 5.2, Primary and Backup Administrators, are members of at least one of the specified security groups.

AD DS Domain	Security Group
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
<add or delete rows as needed>	

Chapter 6 SharePoint Online Email

SharePoint Online will send alerts and notifications via email. A Simple Mail Transfer Protocol (SMTP) server and an outbound email address are required.

section 6.1
SMTP Server

SharePoint Online sends alerts and notifications using an onsite SMTP server for the outbound messages. If it is available, these messages are sent using Exchange Online. Otherwise, you must specify an SMTP server for this role. SharePoint Online only configures SharePoint to route SMTP requests to SMTP services that are accessible from a FQDN. This FQDN can be hosted onsite in your own datacenter/server or provided by the Microsoft Hosted Exchange Service.

> **Important**
> The FQDN cannot be an IP addresses (including VIPs) or a single server name.

Did you purchase Exchange Online? *(Yes or no)*

If you answered “yes,” skip to Section 6.2, Outbound Email Addresses.
If you answered “no,” what on-premises SMTP server should be used? *(Enter SMTP server name here)*
If your SMTP server is on-premises but does not use Microsoft Exchange Server, what is the name of the Active Directory attribute that stores your email address? *(Enter AD attribute name here)*

section 6.2
Outbound Email Addresses

Provide the email addresses you want SharePoint Online to use as the Sender and Reply-To addresses for outbound email messages:

Sender email address - The Sender email address is used in the header of alert messages and identifies the sender of the message: *(Enter Sender email address (for example, sharepoint@contoso.com)*

Reply To email address - The Reply-To email address is the address displayed in the **To** field of a message when a user replies to an alert or notification: *(Enter Reply-To email address (for example, donotreply@contoso.com)*

Chapter 7 Partner Access

Did you plan to use Partner Access? *(Yes or no)*

If you answered “no,” you are finished with the Discovery Questionnaire process.
If you answered “yes,” please fill out the remaining Discovery Questionnaire.

For Partner Access, is the Domain Name Server (DNS) domain of your AD DS resolvable via the Internet? *(Yes or no)*

If it is not, SharePoint Online requires the IP addresses of the DNS servers that can resolve the AD DS name. Provide them in the following table.

DNS Server IP Addresses
(Enter IP address here)
(Enter IP address here)
(Enter IP address here)
(Enter IP address here)
<add or delete rows as needed>

If you intend to use SAML-based partner collaboration, it is strongly recommended you enlist the aid of a claims-based authentication subject-matter expert. See the Microsoft Download Center book “A Guide to Claims-Based Identity and Access Control, Second Edition” (http://www.microsoft.com/en-us/download/details.aspx?id=28362) for more details.

section 7.1 Identifying Partners by Domain or Suffix

SharePoint Online uses unique suffixes (for example, `contoso.com`) or AD DS domains to identify your partner users from your regular employee users when creating reports about partners.

In some cases, there are more suffixes for partners than for employees, so it can be easier to indicate which suffixes do not designate partners. To differentiate between partner and employee identities, provide a list of suffixes or domains (or a mix of both) that corresponds to one or the other in the following table.

> **Important**
> You must indicate if the following list includes partners (and is therefore included in the reports) or it excludes partners (and will be omitted) by answering “yes” or “no” to the following question:
>
> Suffixes/domains in the list include partners *(Yes or no)*

UPN Suffix
(Enter suffix or domain here)
(Enter suffix or domain here)
(Enter suffix or domain here)
(Enter suffix or domain here)
<add or delete rows as needed>

section 7.2 SharePoint Online Partner Access URL

Important
SharePoint Online does not support SAML-based partners' collaboration on your corporate SharePoint Online URLs, such as Portal and Team Sites. As such, partner collaboration requires a dedicated Partner Access URL.

Note
The URL denoted for Partner Access cannot be changed.

Enter a fully qualified domain name (FQDN) in the following table (for example, `contosopartners.sharepoint.net`):

URL[‡‡]	FQDN
Partner Access URL	*(Enter FQDN for Partner Access here)*

section 7.3 Partner Access Authentication Method

Important
You must specify either security group(s) for partners in AD DS or role claim(s) for partners authenticated by a security token service (STS). (See the MSDN article "Security Token Service" (http://msdn.microsoft.com/en-us/library/ee748490.aspx) for more details.) With Windows Claims authentication, use of the same domain for employees and partners is not supported. With SAML Claims authentication, all partner users must share a unique UPN suffix.

If the partner accounts reside in the same Active Directory as your employees, the partner accounts will also be authenticated using AD DS. As such, you need to create a distinct security group to identify and grant specific privilege for these accounts. See Section 7.3.1, AD DS Groups for Partner Access, for more details.

If the partner accounts reside in a different Active Directory of their own, their authentication must be federated by Active Directory Federation Services (AD FS) or any other STS product that is supported by SharePoint Online. See the Microsoft TechNet article "AD FS 2.0 Product Help" (http://technet.microsoft.com/en-us/library/dd727943(v=ws.10).aspx) for more details on AD FS. See Section 7.9.1, Security Token Service to be Used, for more details on supported STS products.

In this scenario, user accounts are identified based on the role claim value that they are identified by during authentication. These role claim values are simple strings (for example, "Partners", "Sales", or "Managers") and are required to grant specific privileges applicable to that group of users. This is analogous to how security groups are recognized in Active Directory. See Section 7.3.2, STS Role Claims for Partner Access, for more details.

Will your partners be authenticated by AD DS or an STS? *(Specify AD DS or STS)*

- If you are using AD DS, complete Section 7.3.1, AD DS Groups for Partner Access.
- If you are using an STS, complete Section 7.3.2, STS Role Claims for Partner Access.

‡‡ All URLs for your SharePoint Online Web applications will share the same FQDN pattern. For example, if your URLs are `*.contoso.net`, then the Partner Access URL must be `https://partner.contoso.net`.
SharePoint Online only supports three-part URLs, like the Partner Access URL example cited in the previous sentence.

section 7.3.1
AD DS Groups for Partner Access

Security groups are used to secure permission policies and deny access to content based on the permissions you specify in Section 7.6, Permission Policies. To avoid giving partners the same permissions and access as employees, specify the domains and security groups your partners belong to in the following table.

AD DS Domain	Security Group
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
<add or delete rows as needed>	

section 7.3.2
STS Role Claims for Partner Access

Your partner-based STS role claims are used to identify all partners, secure your permission policies, and deny access to content based on the permissions you specify in Section 7.6, Permission Policies. To avoid giving partners the same permissions and access as employees, specify the STS role claims your partners belong to in the following table.

STS Role Claim
Example: "Partners"
(Enter STS role claim here)
(Enter STS role claim here)
(Enter STS role claim here)
<add or delete rows as needed>

section 7.4
Partner Access Permissions to SharePoint Online Web Applications

Note
If your partners use SAML for partner collaboration, they will be unable to access Portals, Team Sites, and SkyDrive Pro sites.

For Active Directory authentication, several options exist for granting or restricting access for partner users to each of the three standard Web applications (Portals, Team Sites, and SkyDrive Pro sites). Partners can be:

- Completely blocked from accessing other Web application (recommended).
- Subject to the default policy limits on access for partner users. Refer to Section 7.6.1, Default Permission Policy, for a list of the permissions that are denied by this policy.

Important
The default permission policy prevents partners from being able to create or administer a site collection, limits their permissions, and prevents them from creating SkyDrive Pro sites. You can define a custom policy that creates further limits based on your security policies. The permissions you choose to deny **cannot** be granted by local site collection administrators. **The default permission policy does not grant permissions; it defines what a partner cannot be granted permission to do by local site collection administrators.**

- Subject to custom policy limits on access for partner users. Refer to Appendix A, Custom Permission Policy, for more information.

SharePoint Web Application	Partner Access Level
Portal	*(Specify completely blocked, unlimited access, per default policy, or per custom policy (configure settings in Section 7.6.2, Custom Permission Policy)*
Team Sites	*(Specify completely blocked, unlimited access, per default policy, or per custom policy (configure settings in Section 7.6.2, Custom Permission Policy)*
SkyDrive Pro[§§]	*(Specify completely blocked, unlimited access, per default policy, or per custom policy (configure settings in Section 7.6.2, Custom Permission Policy)*

section 7.5 SkyDrive Pro Policies

By default, partners will be completely restricted from accessing SkyDrive Pro sites. This means partners will see "Access Denied" messages when they click on people's names in SharePoint.

Should partner users be able to view the SkyDrive Pro of employees and other partners (they can view profiles and use social features, such as ratings and tagging)? *(Yes or no)*

- If you answered "no," skip to Section 7.6, Permission Policies,
- If you answered "yes," should partners *also* be given read access to all the personal site content of other users, including shared documents and blogs? *(Yes or no)*
    - If you answered "yes," skip to Section 7.6, Permission Policies.
    - If you answered "no," you must specify how to identify employees who will be granted read access by default.
    - ♦ If you are using AD DS, complete Section 7.5.1, AD DS Security Groups for Allowing Access to Personal Content only to Employees.

[§§] Restricting access to SkyDrive Pro URLs will prevent partners from using some social features, such as tagging. This is covered in further detail in section 7.5, SkyDrive Pro Policies.

section 7.5.1
AD DS Security Groups for Allowing Access to Personal Content only to Employees

Partner users are not allowed to view SkyDrive Pro sites. You need to identify the **employees** who should, by default, be granted read access to personal content.

Specify the AD DS domains and security groups the employees belong to in the following table.

AD DS Domain	Security Group
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
(Enter AD DS domain here)	*(Enter security group here)*
<add or delete rows as needed>	

section 7.6 Permission Policies

section 7.6.1
Default Permission Policy

If you use the default policy, partner users are denied all administrative permissions and are limited to only those permissions that are normally granted to a site collection member. Partners are specifically restricted from exercising the permissions listed in this section as well as creating SkyDrive Pro sites. Even if a site collection administrator grants a partner user these permissions at the site collection level, the default policy will override that local permission at a global level and prevent the partner user from exercising the permission.

The following *list permissions* are denied by the default policy:

- Manage Lists
- Override Check Out
- Approve Items

The following *site permissions* are denied by the default policy:

- Manage Permissions
- View Web Analytics Data
- Create Subsites
- Manage Web Site
- Add and Customize Pages
- Apply Themes and Borders
- Apply Style Sheets

- Create Groups
- Browse Directories
- Enumerate Permissions

section 7.6.2
Custom Permission Policy

If you want to specify custom permission policies, refer to Appendix A, Custom Permission Policy.

Do you plan to use the default permission policy or specify a custom permission policy? *(Use the default permission policy/Specify a custom permission policy)*

If you answered “Use the default permission policy,” skip to Section 7.7, Importing User Profiles from Lightweight Directory Access Protocol Sources (Federated Trust Required).

If you answered “Specify a custom permission policy,” fill out the tables in Appendix A, Custom Permission Policy.

section 7.7
Importing User Profiles from Lightweight Directory Access Protocol Sources (Federated Trust Required)

SAML claims-based users may have user information in several different supported Lightweight Directory Access Protocol (LDAP) sources. This set of instructions details the necessary steps to import and authenticate users through an LDAP-federated trust and an STS product:

- You must host the supported STS product and ensure it is available prior to the Web App deployment by SharePoint Online.
- If you want to use profile synchronization, your directory service must be accessible from the managed network.
- If users will connect from the Internet, the STS product must be publicly accessible from the Internet.
- If users will connect from your corporate network, they require access through Internet proxy servers to Microsoft’s STS in order to be authenticated.

Note
Federation is the collaboration between two domains which are aware of each other’s existence. When customers want their partner users to use the SharePoint Online farm, partner users must have their own Active Directory environment for federation to work correctly. If the partners authenticate and route Internet traffic through a proxy or Microsoft Forefront® United Access Gateway (UAG), they also need Internet connectivity and DNS to communicate and federate requests. The customer takes responsibility for identifying these domains when a federation request is sent by AD FS.

- Windows Claims must always be enabled.

Note
In order to use AD FS with SharePoint Online, you will need to provide the information listed in this section (7.7) of the questionnaire.

A federated trust between your network and SharePoint Online requires the exchange of partner policy files with all of the uniform resource identifiers (URIs), claim types, claim mappings, and other necessary values and verification certificates.

section 7.7.1
Directory Service Used for Profile Import

Which supported directory service are you using? *(Specify one of the following: Active Directory, IBM Tivoli 5.2, Novell eDirectory 8.7.3, SunOne 5.2, Other – unsupported)*

section 7.7.2
Account Information Used for Profile Import

Accounts may be used in more than one forest or domain. An account is required for each forest or domain that does not trust the others. A maximum of eight profile synchronization forests and/or domains is supported.

Note
Specific STS products require specific permissions, as listed below:

- In SunOne, the account requires anonymous access to RootDSE for Read, Write, Compare, and Search permissions, and also Read, Compare, and Search permissions for the `cn=changelog` object.
- In Novell eDirectory, the account requires Browse permissions in the Entry permissions property for the specified tree, and also Read, Write, and Compare permissions in the All Attributes permissions property for the specified tree.
- In IBM Tivoli, the account is required to be a member of an administrative group in order to perform profile synchronization.

To import user profiles from an STS product, provide the domain and account information for each forest and/or domain in the following table.

Important
A separate password-protected Excel spreadsheet will be sent by your deployment consultant to provide the needed password information to Microsoft. A meeting will be scheduled by your deployment consultant to provide you with the password to the protected spreadsheet.

Once you have added the account information and password(s) to the SharePoint Network Accounts tab in the spreadsheet, perform the following steps:

1. Create an email using the following alias for Microsoft O365 SharePoint: O365SPOEP@microsoft.com
2. Enter the following in the Subject line: <<Customer Name>>.xlsx
3. Attach the encrypted <<Customer Name>>.xlsx spreadsheet to the email.

Warning
Do not include the spreadsheet's encryption password in this email.

The password must be:

- Non-expiring.
- A minimum of 15 characters.
- A mix of upper- and lower-case letters and digits, and include at least *one of these* special characters: `@!{}[]`
- You cannot use the following special characters: comma (,), semi-colon (;), or double quote (“), as the SharePoint profile importer cannot process these characters.

Account Name	Password	Port	Provider Name	UID	Full Path of Forest Name	Full Path of Domain Controller Name
(Enter account name here)	*(Send by secure email. DO NOT ENTER HERE)*	*(Specify one of the following: 389, 636, Other (enter here))*	*(Enter provider name here (optional))*	*(Enter UID here (optional))*	*(Enter forest name path here)*	*(Enter domain controller name path here)*
(Enter account name here)	*(Send by secure email. DO NOT ENTER HERE)*	*(Specify one of the following: 389, 636, Other (enter here))*	*(Enter provider name here (optional))*	*(Enter UID here (optional))*	*(Enter forest name path here)*	*(Enter domain controller name path here)*
<add or delete rows as needed>						

Is the DNS domain of your AD DS resolvable via the Internet? *(Yes or no)*

If it is not, SharePoint Online requires the IP addresses of the DNS servers that can resolve the AD DS name.

Note
This process authenticates partner user accounts provisioned in Active Directory that also log on through non-domain computers using the Internet.

DNS Server IP Addresses

(Enter IP address here)
(Enter IP address here)
(Enter IP address here)
(Enter IP address here)
<add or delete rows as needed>

section 7.8 SharePoint Online Permissions for Partner Access

section 7.8.1
Administrators for SharePoint Online Web Application Control

Typically, a few trusted IT pros will control SharePoint Online at the Web application level. Specify the security group that these users are part of in the following table.

Security Group
(Enter security group here)
(Enter security group here)
(Enter security group here)
(Enter security group here)
<add or delete rows as needed>

section 7.8.2
Site Collection Administrators for Partner Access

Provide the credentials of the accounts to be used as primary and backup administrators for each SharePoint Online site collection. These accounts are granted full control of the root site collection, including the ability to grant permissions to other users. To add an account, specify its domain and Username, and then select whether it is to be a primary or backup administrative role. Self-service site creation is enabled for all users by default.

Enter the domain and Username of a primary and a backup site collection administrator for the Partner Access URL in the following table. These values are the mandatory primary and secondary values for Web applications (Portal, Team Sites, and SkyDrive Pro sites).

Site Collection Administrator	Domain\Username or UPN
Primary	*(Enter the domain\Username or UPN)*
Backup	*(Enter the domain\Username or UPN)*

section 7.9 Authenticating Partners Through a Federated Trust

Note
If you are not using SAML authentication, skip to Section 7.10, Claims Store.

section 7.9.1
Security Token Service to be Used

To authenticate users through a federated trust with an STS product, you must use a supported authentication product (and version).

This kind of authentication involves the following requirements:

- Your STS product must issue SAML 1.1 or later.
- All federation identity provider STS certificates (encryption, signing, and Transport Layer Security (TLS)) must be issued by, and chained to, a publicly trusted root authority. For a specific list of such root authorities, see the Microsoft TechNet wiki article “Windows Root Certificate Program - Members List (All CAs)” (http://social.technet.microsoft.com/wiki/contents/articles/2592.aspx).

Important
AD FS consumes multi-value claims as separate name-value pairs, all having the same name. Some SAML-based STS role claims may assert multi-value claims as a single name-value pair with multiple delimited values. Your company is responsible for ensuring that any multi-value claim assertion is done using separate name-value pairs as is required for AD FS.

What STS authentication product are you using? *(Specify one of the following: AD FS, Shibboleth 2.0, Other – unsupported)*

section 7.9.2
Federated Trust Metadata URL

To set up a federated trust with SharePoint Online, you must provide your federation metadata URL. Federation metadata contains information such as the token-signing certificate and the token issuance URL. For example, all information about the SharePoint Online AD FS service is contained in the Federation Metadata URL https://sts.microsoftonline.com/federationmetadata/2007-06/federationmetadata.xml.

Note
Ensure that the certificates used by STS role claims are from established certificate authorities.

Important
Federation metadata URLs must start with *https*.

- Do you require separate PPE and production instances of trust? *(Yes or no)*
- If you answered “yes:”
  - Specify your federation PPE metadata URL: *(Enter federation PPE metadata URL here)*
  - Specify your federation production metadata URL: *(Enter federation production metadata URL here)*
- If you answered “no,” specify your federation metadata URL: *(Enter federation metadata URL here)*

OR

Provide your federation service information only if your STS product does not support the federation metadata URL.

Note
If this information is different for your PPE environment, provide both PPE and production information for the following questions.

- Federation service display name: *(Enter federation service display name here)*
- Federation service URL: *(Enter federation service URL here)*
- Federation service identifier: *(Enter federation service identifier here)*
- Federation token signing cert path: *(Enter federation token signing cert path here)*

Is the DNS domain of your STS resolvable via the Internet? *(Yes or no)*

If you answered “yes,” continue to Section 7.10, Claims Store.

If you answered “no,” provide the IP address of the DNS server: *(Enter DNS server IP address here)*

section 7.10
Claims Store

You can host and populate a claims store for lookup, resolution, and validation of claim values. A claims store, and federated trust between the claims store and the SharePoint Online STS, is required if you want validation when users search for names and other claims using the People Picker control (also referred to as the “enhanced experience”). See the SharePoint Online Partner Access SDK 12.3 (http://go.microsoft.com/?linkid=9825164) for more details. If you cannot access the SDK, please contact your SDM.

Note
The claims store must be a .NET Windows Communication Foundation (WCF) service and encrypted with SSL. Without a claims store, you will receive the out-of-box SharePoint experience for the People Picker control, and SharePoint will not support resolution and validation that a claim value for any given claim type (including roles) is correct for users authenticated by an STS. Consequently it will rely on the value you provide as the claim value.

Important
At this time, authorization settings assigned with the out-of-box experience cannot be preserved when the claims store (also known as the “enhanced experience”) is enabled.

If you plan to use a claims store, what is the URL? *(Enter claims store URL here)*

section 7.11
Partner Access Checklist

Complete this checklist to ensure all Partner Access information has been provided before submitting this document to SharePoint Online.

Chapter 1 - Customer Information

☐ Data provided

Chapter 4 - SharePoint Online Application-Level Configuration

Section 4.3 - Importing User Profiles from Active Directory Domain Services

Are you importing user profiles? ☐Yes ☐No *(if yes, select one of the following)*

either

☐ Section 4.3.1 - Active Directory Groups

or

☐ Section 4.3.2 - Information for Accounts Used to Import User Profiles (Account information and passwords sent to SharePoint Online via Individual Rights Management (IRM) protected email)

Are you filtering imported profiles? ☐Yes ☐No

Chapter 7 - Partner Access

Section 7.1 - Identifying Partners by Domain or Suffix

☐ List includes partners

☐ List excludes partners

Section 7.2 - SharePoint Online Partner Access URL

Is there an URL? ☐Yes ☐No

Section 7.3 - Partner Access Authentication Method *(select one of the following)*

either

☐ Section 7.3.1 - AD DS Groups for Partner Access

or

☐ Section 7.3.2 - STS Role Claims for Partner Access

Section 7.4 - Partner Access Permissions to SharePoint Online Web Applications

☐ Access levels set

Section 7.5 - SkyDrive Pro Policies

Can partners access SkyDrive Pro sites? ☐Yes ☐No

If yes, complete Section 7.5.1 below. If no, skip to Section 7.6.

Section 7.5.1 - AD DS Security Groups for Allowing Access to Personal Content only to Employees

☐ Only to Employees

Section 7.6 - Permission Policies *(select one of the following)*

either

☐ Section 7.6.1 - Default Permission Policy

or

☐ Section 7.6.2 - Custom Permission Policy

If Custom Permission Policy selected

☐ **Appendix A: Custom Permission Policy** completed

Section 7.7 - Importing User Profiles from Lightweight Directory Access Protocol Sources (Federated Trust Required) *(Select all that apply)*

☐ Section 7.7.1 - Directory Service Used for Profile Import

☐ Section 7.7.2 - Account Information Used for Profile Import

(Account information and passwords sent to SharePoint Online via Individual Rights Management (IRM) protected email)

Section 7.8 - SharePoint Online Permissions for Partner Access

Section 7.8.1 - Administrators for SharePoint Online Web Application Control

☐ STS role claim or UPN provided

Section 7.8.2 - Site Collection Administrators for Partner Access

☐ Credentials provided

Section 7.9 - Authenticating Partners Through a Federated Trust *(must be completed if using STS)*

Section 7.9.1 - Security Token Service to be Used

☐ STS product indicated

Section 7.9.2 - Federated Trust Metadata URL

☐ Metadata URL or federated trust information provided

Section 7.10 - Claims Store *(Optional, but recommended)*

Are you using a claims store? ☐Yes ☐No

Appendix A Custom Permission Policy

You can write a custom permission policy in which you specify which permissions a partner user can be eligible for, and then provide a policy where all other permissions are denied. To create a custom policy, select the permission level for each function in each of the following tables.

> **Note**
> Some permissions are interdependent (one permission requires another permission). It is recommended that you test the permission set within a site collection to ensure it grants the desired capabilities.

When you are finished, continue with Section 7.7, IImporting User Profiles from Lightweight Directory Access Protocol Sources (Federated Trust Required).

section A.1 List Permissions

Policy Name	Description	Permit or Deny
Manage Lists	Create and delete lists, add or remove columns in the list, and add or remove public views of a list.	*(Permit or deny)*
Override Check Out	Discard or check in a document that is checked out to another user.	*(Permit or deny)*
Add Items	Add items to lists and documents to document libraries.	*(Permit or deny)*
Edit Items	Edit items in lists, edit documents in document libraries, and customize Web Part pages in document libraries.	*(Permit or deny)*
Delete Items	Delete items from a list or documents from a document library.	*(Permit or deny)*
View Items	View items in lists and documents in document libraries.	*(Permit or deny)*
Approve Items	Approve a minor version of a list item or document.	*(Permit or deny)*
Open Items	View the source of documents with server-side file handlers.	*(Permit or deny)*
View Versions	View past versions of a list item or document.	*(Permit or deny)*
Delete Versions	Delete past versions of a list item or document.	*(Permit or deny)*
Create Alerts	Create alerts.	*(Permit or deny)*
View Application Pages	View forms, views, and applications pages. Enumerate lists.	*(Permit or deny)*

section A.2 Site Permissions

Policy Name	Description	Permit or Deny
Manage Permissions	Create and change permission levels on the Web site, and assign permissions to users and groups.	*(Permit or deny)*
View Web Analytics Data	View reports on Web site usage.	*(Permit or deny)*
Create Subsites	Create sub-sites, such as Team Sites, Meeting Workspace sites, and Document Workspace sites.	*(Permit or deny)*
Manage Web Site	Grants the ability to perform all administration tasks for the Web site, as well as manage content.	*(Permit or deny)*

Policy Name	Description	Permit or Deny
Add and Customize Pages	Add, change, or delete HTML pages or Web Part pages, and edit the Web site using a SharePoint Foundation-compatible editor.	*(Permit or deny)*
Apply Themes and Borders	Apply a theme or borders to the entire Web site.	*(Permit or deny)*
Apply Style Sheets	Apply a style sheet (.css file) to the Web site.	*(Permit or deny)*
Create Groups	Create a group of users that can be used anywhere within the site collection.	*(Permit or deny)*
Browse Directories	Enumerate files and folders in a Web site using SharePoint Designer and Web Distributed Authoring and Versioning (WebDAV) interfaces.	*(Permit or deny)*
View Pages	View pages in a Web site.	*(Permit or deny)*
Enumerate Permissions	Enumerate permissions for the Web site, list, folder, document, or list item.	*(Permit or deny)*
Browse User Information	View information about users on the Web site.	*(Permit or deny)*
Manage Alerts	Manage alerts for all users of the Web site.	*(Permit or deny)*
Use Remote Interfaces	Use Simple Object Access Protocol (SOAP), WebDAV, the Client Object Model or SharePoint Designer interfaces to access the Web site.	*(Permit or deny)*
Use Client Integration Features	Use features that launch client applications. Without this permission, users must work on documents locally and upload their changes.	*(Permit or deny)*
Open	Allows users to open a Web site, list, or folder in order to access items inside that container.	*(Permit or deny)*
Edit Personal User Information	Allow a user to change their own user information, such as adding a picture.	*(Permit or deny)*

section A.3 Personal Permissions

Policy Name	Description	Permit or Deny
Manage Personal Views	Create, change, and delete personal views of lists.	*(Permit or deny)*
Add/Remove Personal Web Parts	Add or remove personal Web Parts on a Web Part page.	*(Permit or deny)*
Update Personal Web Parts	Update Web Parts to display personalized information.	*(Permit or deny)*

Appendix B Required Claims for SharePoint Online

The following claims are required for SharePoint Online. You can send additional claims, and AD FS will forward them on, but the claims listed here are the only ones that SharePoint Online uses. All other claims will be discarded.

Name	Claim Type	Multi-value?	Required?	Example
UPN	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	No	Yes	John.doe@contoso.com
Common Name	http://schemas.xmlsoap.org/claims/CommonName	No	No	John Doe
Given Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	No	No	John
Job Title	http://schemas.microsoftonline.com/federation/customclaims/JobTitle	No	No	CFO
Organization	http://schemas.microsoftonline.com/federation/customclaims/Organization	No	No	Contoso
Role	http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Yes	No	Executives; finance; Team4
SIP	http://schemas.microsoftonline.com/federation/customclaims/SIP	No	No	sip:john.doe@contoso.com
Surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	No	No	Doe
Work Email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	No	No	John.doe@contoso.com
Country	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country	No	No	US
UserType	http://schemas.microsoftonline.com/federation/customclaims/usertype	No	No	FTE