Office 365

Dedicated and ITAR-support Plans

Identity & Provisioning Dedicated Service Description

Applies to: *Office 365 Dedicated - Legacy Platform Releases*

Topic Last Modified: *2015-08-31*

Identity & Provisioning Dedicated Service Description 1

Authentication Services 5
- Active Directory Domain Services 5
  - Active Directory Architecture 6
  - Active Directory Trusts 7
  - Authentication Protocols 8
- Domain Controller Implementation 9
  - Physical Location of Customer Forest Dedicated Domain Controllers 9
  - Configuration of Customer Forest Dedicated Domain Controllers 11
  - Capacity Planning for Customer Forest Dedicated Domain Controllers 13
  - Active Directory Site Requirements 15
  - Domain Controller Considerations for SharePoint Online Customers 15
  - Responsibilities 19
- DNS Namespaces Configuration 20
  - Split-Horizon DNS 21
  - Unsupported DNS Configurations 21
  - Responsibilities 22
- Active Directory Federation Services 23
- Active Directory Rights Management Services 24
- Multi-Factor Authentication 24
- Microsoft Office Client Authentication Services 25

Directory Synchronization and Service Provisioning 25

Microsoft

Synchronization Life Cycle 26
Service Provisioning and Deprovisioning Details 30
Provisioning of Object Types 30
Provisioning of Services 31
Deprovisioning of Services 32
Automatic Service Reconnection After User Domain Moves 33

Service Continuity for Identity and Provisioning Services 34

The identity and provisioning services that are available with Office 365 Dedicated fulfill a critical role to enable and regulate your organization's access to Microsoft cloud-based applications such as Microsoft Exchange Online, Microsoft SharePoint® Online, and Microsoft Lync™ Online. The identity and provisioning services focus primarily on the following key service areas:

- **Authentication services.** Active Directory® authentication services using Integrated Windows® authentication enables users to access Office 365 Dedicated resources via a single sign-on experience. With single sign-on, users can sign in once to receive access to resources such as their Exchange Online mailbox, SharePoint Online sites, or Lync Online profile. Optional Active Directory authentication services include (a) federated authentication to access Exchange Online and SharePoint Online and (b) rights management services to protect email and documents within Exchange Online and SharePoint Online.

- **Directory synchronization and provisioning services.** For user accounts that reside within the Office 365 Dedicated environment, synchronization and provisioning services ensure that user accounts are properly provisioned for the Office 365 resources for which they have a subscription to use. These provisioned user accounts are mail-enabled but are disabled for logon. Two examples of provisioned resources are an Exchange Online mailbox and a Lync Online profile.

This service description presents the authentication, directory synchronization, and provisioning components that Microsoft provides to your organization as part of Office 365 Dedicated and ITAR-support subscription plans.

Notes:

- Unless otherwise indicated, the information in this service description also applies to the International Traffic in Arms Regulations (ITAR-support) version of Office 365.
- Services provided under Office 365 Dedicated and ITAR-support plans are delivered from a Microsoft cloud data center environment. Within the environment, your organization has its own dedicated data center hardware for your core services, access to authentication systems that are common to either all Office 365 Dedicated customers or all Office 365 ITAR-support customers, and access to shared services provided to all Office 365 multi-tenant and dedicated customers (shared services are not applicable to ITAR-support customers).
- The content of this service description represents platform services for existing customers of the Dedicated and ITAR-support plans of Office 365 that utilize the Exchange Server 2013, SharePoint Server 2013, and Lync Server 2013 versions of the cloud offerings. New customers will utilize a newer Office 365 release of each core service. Each new release leverages a common service fabric designed to support either a multi-tenant or dedicated implementation of the service. All existing Office 365 Dedicated customers gradually will be migrated to the new service releases and the new platform services that support each core service. Contact your Microsoft account team for additional information.

The information applies to the following Office 365 Dedicated services:

- **Exchange Online Dedicated**
- **SharePoint Online Dedicated**
- **Lync Online Dedicated**

The intended audience for this information is IT professional level staff with a strong understanding of Active Directory services.

Authentication Services

Authentication is the process of determining whether a user or computer is, in fact, who or what it declares itself to be. There are several methods of authentication. Office 365 Dedicated uses Active Directory authentication technologies developed by Microsoft. Optional multi-factor authentication features also are available.

Your organization's involvement is required to implement an authentication service design for Office 365 Dedicated services. The design must address the following:

- Implementation of an Active Directory Domain Services architecture for Office 365 Dedicated that includes the following:
  - Active Directory trust relationships between your forests (Customer Forest) and the Office 365 Dedicated forest (Microsoft Managed Forest).
  - Use of specific authentication protocols.
  - Customer Forest domain controllers dedicated to servicing the authentication load generated by Office 365 Dedicated services.
  - Implementation of DNS name resolution services.
- Implementation of optional Active Directory Federation Services, Active Directory Rights Management Services, and multi-factor authentication features.

Each of these authentication technologies is described in more detail in the sections that follow.

Active Directory Domain Services

Active Directory Domain Services (AD DS) provide secure, structured, hierarchical data storage for objects in a network such as users, computers, printers, and services. The hierarchical containment structure includes the Active Directory forest, domains in the forest, and organizational units (OUs) in each domain. A server that is running AD DS is called a domain controller. Specific communication protocols are utilized between the domain controllers of an AD DS environment. Specific levels of trust also must be established between forests within your on-premises environment and Office 365 Dedicated.

Active Directory Architecture

The Active Directory architecture for Office 365 Dedicated consists of three types of Active Directory forests: Customer Forests, Microsoft Managed Forests, and Microsoft Management Forests.

Customer Forest

The Customer Forest refers to the Active Directory forests and domains that exist in your environment. The Customer Forest contains identity objects including user objects that can be provisioned to use Office 365 Dedicated services. Your organization chooses and configures the specific users that will be provisioned for services.

The Customer Forest includes domain controllers dedicated to servicing authentication requests generated by an Office 365 Dedicated service. The functional level for all your Active Directory forests and domains must be Windows Server® 2003 or higher. The Customer Forest may contain your user accounts, contacts, security groups, and distribution groups. You own, manage, and maintain the Customer Forest. Microsoft operations personnel do not have access to the Customer Forest unless you have provided test accounts within the forest.

Microsoft Managed Forest

The Microsoft Managed Forest is a single Active Directory forest that is used by Microsoft to deploy and deliver Office 365 Dedicated services to your organization. The Managed Forest resides within the Microsoft network and is completely managed by Microsoft.

When your organization subscribes to Office 365 Dedicated, you are provided with your own Managed Forest. The Managed Forest contains Active Directory objects such as users, groups, and contacts. Each user has a mail-enabled user account in the Managed Forest that is disabled for logon. This user account is provisioned for Exchange Online and Lync Online services.

Microsoft Management Forest

Microsoft Management Forests are single-domain forests that contain user accounts and security groups that are required for administration of the Microsoft managed environments. Multiple Management Forests existing to fulfill operational and security requirements. Microsoft operates Management Forests for organizations that subscribe to Office 365 Dedicated and another separate Management Forest for organizations that subscribe to the U.S. International Traffic in Arms Regulations (ITAR) support offering. Only qualified Microsoft personnel can access the Management Forests; your organization has no access to them.

Office 365 Dedicated administrators must sign-in to the Management Forest to gain access to the Microsoft Managed Forest. Microsoft personnel without credentials to access the Management Forest cannot access the Managed Forest. This policy enhances security for the customer accounts that are contained in the Managed Forest.

Active Directory Trusts

An Active Directory trust is required to enable authentication between your Customer Forest (and any domains) and the Microsoft Managed Forest. The trust serves as the authentication pipeline that allows users in a domain to access Office 365 Dedicated resources (such as a mailbox or SharePoint data) in a Microsoft Managed Forest.

Active Directory trusts are implemented between the Microsoft Managed Forest and the Customer Forest. This enables the single sign-on authentication feature of Office 365 Dedicated. Additional information regarding the creation and management of trusts can be found in Microsoft TechNet article Active Directory Domains and Trusts.

Trust Types

Microsoft determines the Active Directory trust type to use between your organization and the Microsoft managed environment based on an assessment questionnaire that you complete and information that Microsoft collects from you during deployment planning. The following trust configurations are permitted:

- **One-way forest trust.** Your organization is typically required to implement a one-way forest trust in which the Microsoft Managed Forest trusts the Customer Forest. Forest trusts provide support for the Kerberos authentication protocol and logging into Office 365 Dedicated services using alternate user principal name (UPN) suffixes. They also support the use of universal security groups in the Customer Forest that are included on access control lists (ACLs) for resources in the Microsoft Managed Forest.
- **Two-way forest trust with selective authentication enabled.** This type of trust is only implemented when specific service features are enabled such as Active Directory Rights Management Services (AD RMS). For more information, see the Use of Selective Authentication with Two-Way Trusts Only section that follows.

Use of Selective Authentication with Two-Way Trusts Only

Your organization should enable the selective authentication security setting on all two-way trusts from the Customer Forest to the Microsoft Managed Forest. A trust provides a pathway for all authentication requests between the forests. Selective authentication provides Active Directory administrators for the Customer Forest more control over which Microsoft Managed Forest users can access shared resources in the Customer Forest. The increased control is especially important when administrators need to grant access to shared resources in the Customer Forest to a limited set of Office 365 Dedicated users from the Microsoft Managed Forest. For more information on selective authentication, see the TechNet article Security Considerations for Trusts.

Authentication Protocols

Your Office 365 Dedicated users are authenticated by domain controllers in your environment. These Office 365 domain controllers participate in the authentication process by issuing either Kerberos referrals and tickets for applications using the Kerberos protocol or by passing through authentication requests to your domain controllers for applications using the NTLM protocol.

Microsoft does not enforce the use of any one authentication protocol on its domain controllers. The configuration of each Office 365 Dedicated application influences which protocol is used. In practice, both the Kerberos version 5 and NTLM (versions 1 and 2) protocols are available and used within Office 365 Dedicated. The Active Directory architecture is optimized for both protocols. Additional overview information for each protocol can be found in the Microsoft TechNet articles NTLM Overview and Kerberos Authentication Overview.

Microsoft Responsibilities

- Configure the trust in the Microsoft Managed Forest.

Customer Responsibilities

- Configure the trust in the Customer Forest.

Limitations

- **NAT connection restrictions.** Microsoft does not support the implementation of network address translation (NAT) technology between your domain controllers and Microsoft domain controllers. Implementing NAT systems requires a highly specific configuration that is dependent on the networking products used. Even if successfully deployed, NAT systems and devices pose operational risks. They require that you change your NAT configuration when Microsoft modifies its domain controller deployments. Without NAT reconfiguration, Microsoft authentication to the Customer Forest can fail.

Domain Controller Implementation

Your organization must dedicate domain controllers in each Customer Forest to manage the service authentication load generated by Office 365 Dedicated users. This requirement will ensure access to Office 365 Dedicated services is not negatively impacted due to loads introduced by applications not associated with the services. To ensure network latency requirements are met, dedicated domain controllers are required for (a) each customer domain that contains Office 365 users and (b) forest root domains. If you are a SharePoint Online subscriber, special domain controller implementation options are available if you are unable to meet the maximum allowed network latency for the service as described in the next section.

Physical Location of Customer Forest Dedicated Domain Controllers

To provide redundancy, your Customer Forest dedicated domain controllers must be installed in two physical locations for each geographic region where Office 365 Dedicated services are deployed. Geographic regions with Office 365 Dedicated data centers are North America (dedicated and ITAR-support plans), Western Europe (dedicated plans only), and Asia-Pacific (dedicated plans only). Each location must contain dedicated domain controllers for forest root domains as well as for account domains containing Office 365 Dedicated users. The exact locations of the dedicated domain controllers are primarily driven by the requirements of your Office 365 Dedicated service subscriptions as well as the physical location of your data centers.

The following table summarizes the allowed round-trip network latency between the Microsoft Managed Forest domain controllers and the Customer Forest domain controllers for each Office 365 Dedicated service.

Office 365 Dedicated Service	Round-trip Network Latency Threshold
Exchange Online	250 milliseconds
SharePoint Online	40 milliseconds
Lync Online	250 milliseconds

If your organization subscribes to the SharePoint Online service and does not have the ability to achieve the 40 millisecond network latency threshold using domain controllers placed within your on-premises data center, you will be provided with the option to co-locate your dedicated domain controllers in a Office 365 Dedicated data center where the SharePoint Online servers are deployed. See the Domain Controller Considerations for SharePoint Online Customers section for more information.

Note:

The option to co-locate dedicated domain controllers within Office 365 Dedicated data centers is only available for the SharePoint Online service. The domain controllers must be placed in the continental region where the service is provided. If your organization subscribes to Exchange Online or Lync Online *without* SharePoint Online in a geographic service area of Office 365 Dedicated, the dedicated domain controllers must be deployed in two data centers that are managed by your organization and located in the same geographic region as the Exchange Online and Lync Online servers.

Configuration of Customer Forest Dedicated Domain Controllers

Customer Forest dedicated domain controllers must be configured as follows:

- Dedicated domain controllers must run on a version of Windows that supports increased MaxConcurrentApi values to support the volume of NTLM pass-through authentication generated by Office 365 Dedicated users. The minimum supported operating system version is Windows Server 2008 with Service Pack 2 and the hotfix available at KB975363. This hotfix also may be installed on Windows Server 2008 R2 and is included in Windows Server 2008 R2 Service Pack 1. Windows Server 2012 and above also are supported.
- The MaxConcurrentApi registry entry must be set to 150 or greater. For additional background information on this setting, see the Microsoft Support article How to do performance tuning for NTLM authentication by using the MaxConcurrentApi setting.
- NetBIOS over TCP/IP must be disabled on network interface cards.
- Dedicated domain controllers must provide global catalog services to enable clients to authenticate for logon.
- Flexible Single-Master Operations (FSMO) roles must be not be held by dedicated domain controllers. Dedicated domain controllers must not be used beyond the scope of user authentication.

Use of Read-Only Domain Controllers

Installing Customer Forest dedicated domain controllers as read-only domain controllers (RODCs) may seem attractive to your organization, especially when co-location in Microsoft data centers is required. For example, administrative account passwords are not stored on RODCs and sensitive attributes are not replicated to RODCs because of the filtered attribute set (FAS). However, Microsoft does not support use of RODCs as Customer Forest dedicated domain controllers for the following reasons:

- RODCs do not cache passwords for trusted domain objects (TDOs) and are therefore of limited use in cross-domain scenarios.
- Some authentication-related operations can be serviced only by writeable domain controllers.
- Placing more than one RODC in the same Active Directory site leads to increased replication traffic over the WAN.

The main technical barrier for co-located RODCs is that RODCs never cache passwords for a trusted domain object (TDO). Therefore, writeable domain controllers are required to service cross-domain requests that need access to TDO passwords (such as setting up a secure channel between domain controllers in trusting and trusted domains) as well as encryption and decryption of Kerberos Ticket Granting Service (TGS) requests. In the Office 365 Dedicated environment, this means that domain controllers in a managed environment would not be able to establish secure channels or pass through NTLM authentication requests to RODCs in the customer environment. This effectively rules out the use of RODCs because a significant portion of authentication takes place using NTLM.

A further consideration is that dedicated Active Directory sites in the Customer Forest typically contain more than one domain controller to handle the authentication load and provide redundancy. Because RODCs perform inbound replication only from a writeable domain controller, they cannot act as replication bridgeheads; thus, Active Directory data would have to be replicated over the WAN to each co-located RODC.

Capacity Planning for Customer Forest Dedicated Domain Controllers

It is your responsibility to ensure that your dedicated domain controllers have adequate capacity to handle the authentication load generated by Office 365 Dedicated users. Office 365 Dedicated personnel of Microsoft are not able to access Customer Forest domain controllers or monitor their performance. You must monitor your authentication load and, should it be required, add additional capacity for domain controllers to sustain the load.

Note:

The TechNet article Capacity Planning for Active Directory Domain Services provides generic information regarding performance monitoring and sizing of domain controllers and can assist you in determining the configuration of domain controller hardware for components not explicitly mentioned below (for example, processor, disk, and network components).

Based upon working closely with existing Office 365 Dedicated customers, Microsoft has developed a set of requirements and guidelines in order to assist you in the initial capacity planning of an Office 365 Dedicated deployment. The following requirements apply to each physical location where Customer Forest Dedicated domain controllers will be installed.

- A minimum of two (2) dedicated domain controllers is required for each account domain containing Office 365 Dedicated users.
- A minimum of two (2) dedicated domain controllers is required for the forest root domain.
- The recommendations below provide additional guidelines to assist you in initial capacity planning for large forests. You also should factor future growth plans into initial sizing efforts.
- For each Customer Forest domain that contains more than 50,000 Office 365 Dedicated users, it is recommended to add one (1) dedicated domain controller (per location) for every 25,000 users. For example, if a domain contains between 50-75,000 users, deploy three (3) dedicated domain controllers; if a domain contains 75-100,000 users, deploy four (4) dedicated domain controllers, etc.

- For forest root domains, it is recommended that the minimum number of dedicated domain controllers in the forest root domain equal the number of dedicated domain controllers in the largest child domain (that is, the child domain with the highest number of dedicated domain controllers). For example, if the largest child account domain has three (3) dedicated domain controllers, the forest root domain should also have a minimum of three (3) dedicated domain controllers. The purpose of this recommendation is to ensure that there is a one-to-one secure channel mapping between forest root domain controllers and child domain controllers. The same principle applies for other parent/child domain relationships within the Customer Forest.

Note:

Your organization is responsible for ensuring that secure channel mappings from trusting to trusted domain controllers in the Customer Forest are evenly distributed. As described in Microsoft TechNet, the nltest tool can be used to reset secure channels on specific domain controllers.

For optimal performance, dedicated domain controllers should have enough memory (RAM) to contain the entire Active Directory database file (NTDS.DIT) plus fulfill the requirements of the operating system and other installed software such as antivirus and systems management agents. Typically, allocating memory based on the size of the NTDS.DIT file plus 4-6 GB is sufficient.

Active Directory Site Requirements

In order to ensure that Microsoft Managed Forest domain controllers use the Customer Forest dedicated domain controllers for authentication, your organization must create Active Directory sites in the Customer Forest with the same names as the Active Directory sites in the Managed Forest and configure the dedicated domain controllers to service the new sites. A typical Office 365 Dedicated deployment requires that you create two sites in Active Directory. Microsoft will provide a list of sites for you to create as part of the Office 365 Dedicated deployment process.

Creating matching Active Directory site names enables efficient domain controller location due to the way the Net Logon service uses DNS records as part of the domain controller locator process. To locate a domain controller in the Customer Forest, the locator on a Microsoft Managed Forest domain controller initiates a site-specific DNS query. The site name that is used for the query is the name of a site in the Microsoft Managed Forest. However, the domain part of the DNS query uses the Customer Forest name. If the site-specific record does not exist because the site name portion does not match, the DNS server for the Customer Forest sends a response to the DNS server in the Microsoft Managed Forest indicating that an appropriate match cannot be found. When this occurs, the Microsoft Managed Forest domain controller sends another DNS query that does not specify any site information.

After an SRV record is returned, the Net Logon service on the Microsoft Managed Forest domain controller will send an LDAP UDP search request (an LDAP ping) to the Customer Forest domain controllers that registered the records. The first Customer Forest domain controller to respond will be used for subsequent operations. If a site-specific record is not returned, this could result in a Customer Forest domain controller being chosen in a distant location with high latency and therefore negatively impact the service.

Domain Controller Considerations for SharePoint Online Customers

As described in the Configuration of Customer Forest Dedicated Domain Controllers section, a subscription to the SharePoint Online service requires network latency between your data centers and the Office 365 Dedicated data centers to be no greater than 40 milliseconds. Microsoft will assist with obtaining network latency measurements to share with you. Test results either before or after the deployment of SharePoint Online that indicate the latency threshold is consistently exceeding the threshold maximum will require the implementation of an alternative domain controller design for your organization.

If you cannot produce a plan within five (5) business days to resolve the increased network latency, Microsoft will initiate the design and deployment of co-located domain controllers for your use at the specific Microsoft data centers used to provide the SharePoint Online service. The design and deployment process is estimated to require 8 - 10 weeks to implement.

The following conditions apply to network latency mitigation efforts:

- Should the need to co-locate customer domain controllers arise, Microsoft will provide four (4) physical servers for a customer to configure as co-located domain controllers. The servers are procured by Microsoft and will meet the Microsoft hardware design standard. Your organization will be responsible for configuring each domain controller as either a virtual server (using the virtualization technology of your choice) or as physical domain controller. Strongly recommended is the use of a virtualization technology (for example, Microsoft Hyper-V) to increase the density of domain controllers installed per physical server—especially if multiple domains must be accommodated. The table that follows describes implementation options for the domain controllers.
- If Microsoft procures hardware as a result of a decision made to co-locate customer domain controllers and the network issue is resolved before the hardware is delivered, Microsoft will proceed to deploy the servers after delivery and maintain them in the data center as backup servers.
- In a scenario where some domain controllers do not meet the latency requirement while others do, the domain controllers that do not meet the criteria must be co-located in a Microsoft data center. The domain controllers that meet the latency criteria do not need to be co-located.

Option	Summary	Overview	Appropriate Customers
Customer-deployed virtualization (recommended)	Customers deploy domain controllers on a virtualization technology of their choice and manage both the virtual machines (VMs) and the host servers.	Microsoft provides four physical servers: two in the primary and two in the secondary data center. Customers deploy the virtualization technology of their choice. Customers manage the host machine and VMs. Customers deploy their own virtual design and divide host resource among VMs as needed to meet proper authentication requirements.	Customers with multiple domains and/ or forests. Customers who want to run their choice of virtual technologies based on their own design.

Option	Summary	Overview	Appropriate Customers
Customer-deployed with no virtualization (not recommended in most circumstances)	Customers deploy domain controllers directly on physical hardware	Microsoft provides four physical servers: two in the primary and two in the secondary data center. Customers manage the server. Customers have only one Active Directory domain per server. Customers that have more than one Active Directory domain with users consuming Office 365 Dedicated services will incur additional hardware costs and monthly fees.	Customers with very large domain controllers, and a single Active Directory domain. *Note*: This option is not recommended for any customer with more than one Active Directory domain, as this configuration would require additional servers to be deployed.

Important

- The domain controller co-location requirement is not intended for authentication redundancy or to mitigate the loss of connectivity to the customer network.
- You will be responsible for operational management of the domain controller servers. Microsoft will provide hardware and data center support for the purpose of hardware life-cycle management or to address a specific request from your organization for support assistance. Microsoft will not at any time have administrative access to your co-located domain controllers.

- For each physical server that is required in excess of the four (4) provided by Microsoft, you will incur a monthly service charge. The charge covers hardware, hosting costs, and break-fix support. An additional monthly service charge may be incurred if data center resources in excess of those provided for a base Microsoft hardware configuration are required.

Responsibilities

Microsoft Responsibilities

- Assist your organization with identifying network latency non-compliance between Microsoft domain controllers and customer domain controllers.
- Assist your organization with resolution of network latency issues, if requested, by providing network monitoring data as your organization directs issue resolution.
- If you cannot resolve the network latency issue within five (5) business days, Microsoft will address the following:
    - Arrange to provide four (4) co-located physical servers for use as dedicated domain controllers (virtual or physical) by your organization.
    - Configure integrated lights-out (iLO) remote management for the domain controller servers and connect the servers to your VLAN.
    - Provide hardware break-fix support for the newly installed domain controller servers at your request.

Customer Responsibilities

- Monitor network latency between your on-premises domain controllers and Microsoft domain controllers.
- Immediately address any network latency increase that exceeds Microsoft defined thresholds for domain controllers located on-premises or produce a plan to remediate the problem within five (5) business days.
- If the network latency issue cannot be resolved within five (5) business days, address the following:
    - Collaborate with Microsoft to develop and implement a solution to co-locate dedicated domain controllers at specific Microsoft data centers.

- On the dedicated domain controller hardware provided by Microsoft, install and configure each domain controller operating environment (that is, a dedicated operating system or a virtualized configuration).
- Acquire licenses for all software to be installed on the co-located domain controllers.
- Monitor the performance of the co-located domain controllers to ensure that the number of domain controllers is sufficient to meet the authentication demands of the Office 365 Dedicated services.
- Update the Active Directory sites and subnet configuration in each Customer Forest.
- Manage the domain controllers remotely and provide monitoring, antivirus updates, and software updates for all physical servers. The same management responsibilities apply if you choose to run the domain controllers on a virtualization technology.

DNS Namespaces Configuration

DNS name resolution across Microsoft and your organization's namespaces is required for Active Directory authentication and for client access to specific Office 365 Dedicated services. In order to set up Active Directory trusts, it is necessary for domain controllers in the Microsoft Managed Forest to resolve names in the Customer Forest and vice versa. To fulfill this requirement, Microsoft will request that you provide a list of DNS servers that can resolve your Active Directory domain names and use the list of names to establish conditional forwarders to these DNS servers. Similarly, Microsoft will provide you with a list of DNS servers that can resolve names in the Microsoft Managed Forest and you will need to configure their DNS servers to conditionally forward requests to Microsoft DNS servers.

Depending upon which Office 365 services your organization subscribes to, it will be necessary for you to establish conditional forwarders to Microsoft DNS servers to resolve names in additional Microsoft-owned namespaces that are not publicly resolvable via the Internet.

Availability Requirements

Microsoft recommends that you host your DNS solution on reliable hardware that is designed for high availability. In addition, these DNS servers must be geographically distributed and have redundant ingress/egress paths through which the Microsoft DNS servers can forward requests.

Split-Horizon DNS

Split-horizon DNS—also called *split brain* DNS—describes a common configuration that allows a single DNS name to be resolved to differing IP addresses depending on the location of the client computer.

Exchange Online Dedicated requires that customers access the service using names in customer-owned domains. Thus, you must implement split-horizon DNS for the domain name used to access Exchange Online.

It is recommended that you choose a domain name for hosting split horizon DNS records related to Exchange Online which is not used by other applications. A common approach is to use a dedicated subdomain of your main domain. For example, if the primary domain of a customer is contoso.com, a subdomain such as o365.contoso.com can be used to host records for accessing online services. The advantage of using a dedicated subdomain is that a customer can make changes to the configuration of the DNS zone for the domain without affecting other applications.

Unsupported DNS Configurations

The sections below describe DNS configurations that are not supported with Office 365 Dedicated networking configurations.

Single-Label Domain Names

Microsoft does not support trusts to your account domains or forest root domains that use single-label domain (SLD) names. SLDs are DNS names that do not contain a suffix such as .com, .corp, .net, or .org. For example, “contoso” is an SLD and therefore is not supported; however, “contoso.com” and “contoso.local” are not SLDs and therefore are supported.

Although Active Directory and DNS currently support single-label DNS names, not all Office 365 Dedicated services support them and therefore they cannot be used. Organizations that use SLD names must rename these domains prior to transitioning to Office 365 Dedicated services.

Zone Transfers

Zone transfers are not supported by Microsoft or between Microsoft and DNS servers. This limitation is primarily due to the additional complexity of the bilateral configuration that is necessary to secure zone transfers.

Setting up zone transfers to your DNS servers outside of a Microsoft Managed Forest would require that a full list of your DNS server IP addresses be maintained on the managed DNS servers.

Responsibilities

Microsoft Responsibilities

- Implement the DNS solution for your organization by completing all the necessary namespace configuration changes required to successfully integrate your network with the Microsoft networks. The work includes, for example, adding forwarders for your specific internal namespaces.
- Consult with your organization in making changes to the DNS configuration.

Customer Responsibilities

- Forward DNS requests for Microsoft-owned internal namespaces to the defined Microsoft DNS servers.
- Provide Microsoft with a list of highly available, geographically-dispersed, internal DNS servers that can resolve all the accessible servers for your organization.
- Address implementation of split-horizon (or split-brain) DNS configurations.
- Avoid the implementation of single-label domain names and zone transfers.

Active Directory Federation Services

Microsoft provides claims-based authentication within Office 365 Dedicated to support the Multi-Factor Authentication feature of Exchange Online Dedicated and the Partner Access feature of SharePoint Online Dedicated. Claims-based authentication is the process of authenticating a user based on a set of claims contained in a trusted token. Claims-aware applications such as Exchange Online and SharePoint Online are claims consumers and these applications will trust tokens provided exclusively by the Office 365 Dedicated federation service.

Multi-Factor Authentication for Exchange Online involves the acceptance of multiple proofs (for example, password, smart card, security question answers, or biometric indicator) to confirm user identity. The feature is implemented using the Office 365 Dedicated Federation Hub in conjunction with a customer-hosted Secure Token Server (STS) and customer-selected third party MFA solution(s). The multi-factor authentication feature is only available with the Exchange 2013 offering of Exchange Online Dedicated and only can be used with Outlook Web App (OWA).

The Partner Access feature for SharePoint Online allows your organization to authenticate users from multiple partner organizations and to permit these users to remotely access SharePoint Online sites and applications through a web-based single sign-on (SSO) experience. The feature enables you and your partners to collaborate, communicate, and share information in a secure way.

The Office 365 Dedicated Federation Hub is an Active Directory Federation Services (AD FS) version 2.0 system that is available as a shared service for all Office 365 Dedicated customers (a separate Federation Hub is available for all ITAR-support plan customers). The Federation Hub utilizes WS-* protocols to support federated claims-based authentication. The AD FS 2.0 federation service provided on Windows Server technology is a highly secure, highly extensible, identity access solution.

Microsoft Responsibilities

- Within Microsoft Office 365 Dedicated and ITAR-support data centers, deploy and manage AD FS servers in federation server and proxy server roles to provide the Federation Hub shared service.
- Within Microsoft Office 365 Dedicated and ITAR-support data centers, deploy and manage AD FS database servers to store configuration information.

- Deploy certificates to sign and validate the Security Assertion Markup Language (SAML) tokens as well as encrypt traffic between the clients and the servers.

Customer Responsibilities

- Provide access to an STS system for your environment that conforms to the Web Services Federation Language (WS-Federation) specification and issues security tokens conforming to Secure Access Markup Language (SAML) 1.1 or later.
- Establish federation trust between the Office 365 Dedicated Federation Hub and your STS system.
- Manage identity claim providers.
- Manage indirect federation with partners.

Active Directory Rights Management Services

The use of Active Directory Rights Management Services (AD RMS) to support the Information Rights Management (IRM) is available within Exchange Online Dedicated and SharePoint Online Dedicated. See the Service Description for each service for additional implementation information.

Multi-Factor Authentication

Typical authentication practices that require only a password to access resources may not provide the appropriate level of protection for information that is sensitive or vulnerable. Multi-factor authentication (MFA) is an authentication method that applies a stronger means of identifying the user. It requires users to submit a combination of the following three types of identify proofs:

- Something known (such as a password or PIN)
- Something possessed (such as a smart card)
- Something unique about the user's appearance or person (such as a fingerprint)

MFA is an optional feature available with Office 365 Dedicated and ITAR-support plans. For more information regarding the MFA implementation for Exchange Online Dedicated, see the *Multi-Factor Authentication for Outlook Web App* in the Exchange Online Dedicated Service Description.

Microsoft Office Client Authentication Services

Office 365 Dedicated provides the ability to automate the licensing of Office application suites for thick clients and mobile clients in conjunction with the use a standard Office 365 tenant. The Click-to-Run service performs license validation and in addition offers a streaming method to deliver the Office Professional Plus 2013 application suite to thick clients. For the Office Mobile suites available for Android and Apple third party mobile products, an automated licensing feature is available to support the activation of the Office suite that has been downloaded to the device by the user.

To utilize either service, contact your Microsoft Service Delivery Manager to request activation.

Directory Synchronization and Service Provisioning

To provision services for Office 365 Dedicated users, Microsoft requires that a mail-enabled user account that is disabled for logon be created for each user in the Microsoft Managed Forest. The system that performs this task is called the Microsoft Managed Solutions Service Provisioning Provider (MMSSPP). The MMSSPP system name is commonly referred to as “Mississippi.”

Built on Microsoft Forefront Identity Manager (FIM) 2010, MMSSPP enables directory synchronization and automated service provisioning between your Customer Forest and the Microsoft Managed Forest. MMSSPP reads user account and other identity data (object attributes) from the Customer Forest, creates logon disabled copies of the user accounts in the Microsoft Managed Forest via synchronization, and then provisions services for those user accounts in the Microsoft Managed Forest.

MMSSPP does not support synchronization from any source directory other than Active Directory. The following describes the key characteristics of MMSSPP:

- **Your directory data is authoritative.** The user account and other identity data that resides in the Customer Forest is the source of all information that is synchronized by MMSSPP to the Microsoft Managed Forest. MMSSPP only reads Active Directory data from your domains that are within scope of Office 365 Dedicated subscriptions.

- **MMSSPP associates an identity object with its objectGUID value in the Customer Forest.** As long as the objectGUID does not change, MMSSPP can re-establish provisioning services related to the object if it is accidentally moved out-of-scope or moved across domains. The objectGUID value is only changed when a new object is created for the same user or if an object is moved across forests. If the objectGUID is altered (for example, a new object is created to represent that identity), MMSSPP can automatically reconnect the managed services to this object utilizing the Automated Services Reconnection (ASR) feature. For more information regarding the format of the objectGUID, see the MSDN article Object-Guid attribute.
- **Directory synchronization and provisioning is an integrated process.** MMSSPP synchronizes a defined set of Active Directory attributes for each identity object (users, groups, contacts). After MMSSPP provisions objects that are in scope from the Customer Forest to the Microsoft managed domain, it automatically provisions or deprovisions services for users that meet specific conditions based on the attribute values of the on-premises Active Directory objects.
- **Customer Forest objects must be in the appropriate state.** Your organization must ensure that Active Directory objects in the Customer Forest meet the requirements for synchronization. If not, objects will be in a synchronization error state that will stop the flow of any changes made to the object.
- **MMSSPP is utilized only by the Exchange Online and Lync Online services.** If you are subscribed only to SharePoint Online services, your organization will not have MMSSPP deployed.

Your organization is provided with the *MMSSPP Customer Deployment Guide* prior to the Office 365 Dedicated onboarding process. The guide contains a checklist of requirements that you must complete. The MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site provides access to all available reference documentation.

Customer Responsibility

- Complete the MMSSPP configuration checklist in the MMSSPP Customer Deployment Guide.

Synchronization Life Cycle

The following are the three phases in the MMSSPP synchronization life cycle.

- **Pre-synchronization.** This phase includes validation of your directory and service provisioning plan, and cleanup of Active Directory objects in your Customer Forest that are in scope of MMSSPP.
- **Onboarding.** This phase covers work to connect your networks and forests to the Office 365 Dedicated environment and completion of the initial directory synchronization. Synchronization errors may necessitate additional rounds of cleanup before your deployment reaches the Service Ready milestone.
- **Run State.** This phase includes work to keep the synchronization process healthy and the requests to make configuration changes and design changes. There are two sub-phases in the Run State phase:
    - *Coexistence*. Migration of mailboxes begins and your on-premises messaging system remains in place.
    - *Post-migration*. Migrations are complete for all users and you have decommissioned the on-premises messaging system.

There are several key activities that occur in your environment during the pre-synchronization phase. Included are the segregation of duplicate identities and completion of domain or forest consolidations. Your organization also must ensure that Active Directory objects in scope for MMSSPP are in the appropriate state. For more information about having objects in the appropriate state, see the Synchronization Errors section.

During the onboarding phase, the initial MMSSPP synchronization reads your on-premises identity data and creates a copy in the Active Directory of the Microsoft Managed Forest. MMSSPP utilizes a service account to read from your Active Directory domains.

MMSSPP synchronization is based on set of organizational units (OUs) that you select. The tool can filter out objects based on an attribute-value set. During the initial synchronization, MMSSPP provisions a copy of objects that you have selected to be in scope of Office 365 Dedicated service entitlements. The MMSSPP synchronization engine ensures that the objects provisioned in the Managed Forest correspond to the objects in the Customer Forest. It is important to understand that the copies of user accounts are enabled for messaging and Lync Online services but are disabled for logon purposes.

During Run State, MMSSPP synchronizes only incremental changes to the in scope object after the initial synchronization.

Object Attributes

MMSSPP synchronizes only a defined set of Active Directory attributes for each identity object in the customer directory. MMSSPP does not synchronize custom attributes such as attributes unique to your directory that are created by extending the Active Directory schema. Detailed information about the synchronization process and rules can be found in the *MMSSPP Identity Synchronization Handbook*, which is available from the Microsoft Service Delivery Manager.

Synchronization Errors

When you do not have Active Directory objects in the appropriate state for MMSSPP synchronization, you will find that those objects produce synchronization errors. MMSSPP cannot make any attribute updates or provision services for objects that are in a synchronization error state.

Although there are several causes for objects being in a synchronization error state, a common cause is when two or more objects have duplicate mail or proxy addresses. MMSSPP stops syncing changes for any objects that are in a synchronization error state, which can result in stale data.

By default, synchronization error reports are sent to your organization on a daily basis. You are responsible for remediating these errors immediately. Failure to do so can result in the following issues:

- New-hire mailbox provisioning might fail if the object is in a misconfigured state.
- Mailbox migrations might fail for objects that are in a misconfigured state.
- Your updates to Global Address List (GAL) information cannot synchronize to the Office 365 Dedicated directory while the object is in a misconfigured state. If the phone number of a user with a synchronization error is changed, for example, the updated number is not synchronized to the Office 365 Dedicated hosted GAL.
- Members of a group can be missing in the GAL when MMSSPP is upgraded to a new major version if user objects that were in a synchronization error state existed before the version upgrade. The objects will no longer appear as members of any groups in the Office 365 Dedicated hosted GAL.

Synchronization Intervals

Following the initial directory synchronization, incremental synchronizations will occur approximately every 30 minutes. The timeframe for completing a synchronization cycle can range from 1 minute to a several hours. The cycle completion time depends upon the following:

- Number of attribute and object changes made prior to the start of the synchronization cycle.
- Number of synchronization errors.
- Number of group membership changes.

Object Change Threshold

You can make any number of changes to your directory objects that are in scope of MMSSPP; however, MMSSPP has a built-in feature that stops synchronization of certain types of changes if the number of those changes reaches a specific threshold. These thresholds are set by your organization at the time of deployment and are put in place to safeguard you the event that a bulk change was made in error.

There are two types of changes for which thresholds are set:

- **Object attribute change.** This threshold setting applies when you makes an attribute change to a very large number of objects and, if the change was not intended, it could have undesired consequence to delivery of Office 365 Dedicated services.
- **Object deletions.** This threshold setting applies when you accidentally move a large number of objects to an OU that is not in MMSSPP scope or deletes an OU and would trigger the corresponding managed objects to be deleted.

In a situation where you must make a bulk change that crosses one of these thresholds, you can file a Configuration Request with Microsoft to temporarily disable the threshold.

Synchronization Support for Multiple Customer Forests

MMSSPP supports synchronization of your Active Directory identity objects from multiple customer Active Directory forests to the Microsoft Managed Forest under the following conditions:

- **All attributes are contained in the user logon account.** Your logon account must contain all attributes that are required to be synchronized to the Managed Forest. In other words, MMSSPP cannot selectively synchronize attribute values from different objects in different forests for the same user and merge them in the Microsoft Managed Forest directory.
- **There are no duplicate objects.** Duplicate identity objects must not be in scope of MMSSPP synchronization within the OUs contained in the Customer Forests. MMSSPP defines a duplicate identity as any object that has an SMTP address value within the (a) mail address,

(b) primary SMTP proxy address, or (c) secondary SMTP proxy address attribute that also appears in any of these three address attributes within another object.

- **Group objects are handled in a specified way.** Groups that contain members from Active Directory forests other than where the group object resides must be handled in a specific manner. For more details, see the *MMSSPP Customer Deployment Guide* available within the MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site.

Service Provisioning and Deprovisioning Details

The ability of MMSSPP to provision and deprovision objects is described in the following sections.

Provisioning of Object Types

MMSSPP provisions the following object types from your Customer Forest:

- **User objects** that reside in a source OU of your Customer Forest are provisioned as logon-disabled user objects in the Microsoft Managed Forest. MMSSPP does not provision an identity-only object. The user object must include a mail address in order for the synchronization to occur.
- **Contact objects** that are created in your Customer Forest are provisioned as contact objects in the Managed Forest.
- **Distribution groups** that are created in your Customer Forest are provisioned as distribution groups in the Managed Forest. Your organization is responsible for managing membership in these groups.
- **Mail-enabled security groups** that are created in your Customer Forest (groups with a mail attribute value) are provisioned as security groups in the Managed Forest. Your organization is responsible for managing membership in these groups.

In addition, MMSSPP ensures that all objects that qualify as mail-enabled objects are included in the online address book.

Provisioning of Services

MMSSPP provisions Exchange Online and Lync Online services. It does not synchronize objects or attributes specific to SharePoint Online services; MMSSPP is not required if your organization subscribes only to SharePoint Online.

MMSSPP has the ability to provision services based on a set of conditions such as the presence of the mail attribute or a single explicit rule (for example, extensionaatribute1=createMSOmailbox).

MMSSPP automates provisioning and deprovisioning actions for the following:

- **User mailboxes.** MMSSPP has the ability to automatically provision mailboxes for new users and for resources such as conference rooms. The following rules for automatic provisioning are applied:
  - **Default Provisioning Rule.** If specific conditions are true, MMSSPP will provision the mailbox.
  - **Explicit Provisioning Rule.** If a specific attribute has a specific value, only then will MMSSPP provision a mailbox (for example, extenstionattribute1=createMSOmbx).
  - **New-Hire Mailbox Provisioning Rule.** This rule is only enabled after all of your on-premises mailboxes are migrated. Once enabled, creating an on-premises mail-enabled user with mail value equal to a proxy having an SMTP domain in the inclusion list will result in MMSSPP provisioning a managed mailbox.
- **Lync Online users.** MMSSPP and the Lync Online auto-provisioning service operate in concert to offer automated per-user provisioning of Lync Online feature entitlements.

Note:

The *Office 365 Dedicated & ITAR-support Plans Provisioning Handbook* describes scenarios for provisioning all object and service entitlements. The handbook is available within the MMSSPP & Provisioning Tools area of Office 365 Dedicated & ITAR-support plans Extranet site.

Deprovisioning of Services

MMSSPP deprovisions identity objects if the deprovisioning criteria set during the deployment are met. For compliance management reasons, MMSSPP also will block deprovisioning for user accounts placed on litigation hold.

Moving Objects Out of Scope

If you move an identity object out of scope of MMSSPP synchronization, the object will be deprovisioned and all services (if any) will be disconnected. The mailbox object can be reconnected within the default retention period of 30 days. The Lync Online IM profile cannot be reconnected unless the automatic service reconnection (ASR) feature is utilized within the pending deletion threshold for your organization. This threshold is established by your organization and the default is 1 day. These same principles apply if you delete an identity object. If a logon action disables a user object, there is no effect on the object in the Microsoft Managed Forest.

Explicit Deprovisioning Rules

If you want to remove service entitlements but not delete the identity object completely, you should consult the deprovisioning rules selected for each service at the time of deployment and set the appropriate Exchange Online mailbox type information or Lync Online provisioning attribute values. Setting the Mailbox deprovisioning value (for example, extenstionaatribute1=removeMSOmailbox) will, for example, deprovision the managed mailbox Litigation Hold Deprovisioning Block.

Litigation Hold Deprovisioning Block

When Litigation Hold is enabled on an Exchange Online mailbox, MMSSPP will not delete the managed object or the Exchange Online mailbox associated with the object. The deletion block applies following your action to delete the on-premises user object, move the on-premises user object out of scope, or set the mailbox deprovisioning string. For all cases, MMSSPP will issue a synchronization error.

Automatic Service Reconnection After User Domain Moves

MMSSPP supports automatic service reconnection (ASR). This feature enables the reconnection of Office 365 Dedicated users to their provisioned services, the reconnection of contact or group objects, or the reconnection of Office 365 Dedicated services to a new object following the creation of the new object within your on-premises environment (for example, when a logon account is moved from one Customer Forest to another). With minimal preliminary work, you can automatically reconnect a user to their Exchange Online mailbox, BlackBerry services, SharePoint Online sites, Lync Online profile, or other provisioned service after the user is moved to another forest.

The automatic service reconnection capability is useful in scenarios where you are performing large forest consolidations or when you must move all your users to a new forest. The reconnection feature is applicable to any typical cross-forest move scenario. If the mailbox of a user object is on litigation hold prior to the move of the object to another domain, litigation hold settings will be re-established when the reconnection action is executed.

Service Continuity for Identity and Provisioning Services

Identity and provisioning services for Office 365 Dedicated and ITAR-support plans are hosted at enterprise-level Microsoft data centers designed to deliver highly available and highly resilient online services. Circumstances including hardware failures, natural disasters, and human error can impact service availability. To address this concern, service continuity management processes are employed to manage risks and to ensure that the IT infrastructure for Office 365 services is capable of providing continuing services if normal availability solutions fail.

For the identity and provisioning suite of services, service continuity resiliency measures are based upon the design of each service and the stated Recovery Time Objective (RTO) commitments for the principal Office 365 service (Exchange Online, SharePoint Online, or Lync Online) being supported. For AD RMS, all multi-factor authentication services, and directory synchronization and service provisioning services, an RTO commitment does not apply.

To view service continuity information for a particular Office 365 Dedicated service, refer to the service descriptions for Exchange Online Dedicated, SharePoint Online Dedicated, or Lync Online Dedicated.