CITRIX

App Orchestration 2.0

Credentials Used in the App Orchestration Environment

Prepared by: Andy Zhu

Version: 1.0

Last Updated: December 9, 2013

Contents

Overview

In a typical App Orchestration deployment, many different credentials are involved. There are the credentials used to install and configure the App Orchestration configuration server and the credentials used to migrate a Delivery Site into the App Orchestration environment. You could simply use a domain administrator account for all the credentials required in your App Orchestration deployment. However, as part of security best practice, we recommend you use the least privileged account necessary to perform each action.

App Orchestration requires credentials for the following operations.

- Installing and configuring the App Orchestration configuration server.
- Managing the shared resource domain and the tenant resource domain.
- Creating, migrating, and managing Delivery Sites.
- Creating Delivery Site databases.
- Accessing the Citrix Product Depot.
- Installing software on machines.

This document lists, for each set of credentials, the stage at which the credentials are introduced into the App Orchestration deployment process and the actions they are used to perform. In addition, recommendations on the minimum permissions required for each of these credentials are given.

App Orchestration configuration server installation/configuration credentials

Where specified

You use this domain account to log on to the App Orchestration configuration server locally to perform the installation and configuration.

Actions performed using these credentials

This account is used for the following functions.

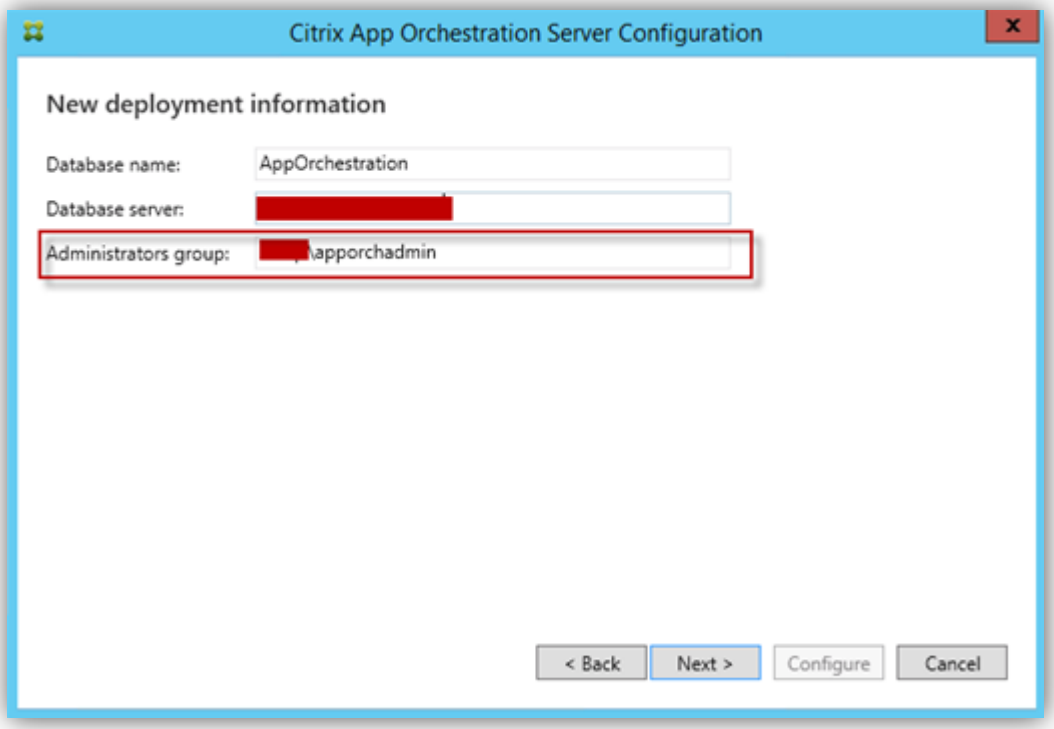
- Installing the App Orchestration configuration server binaries.
- Configuring the App Orchestration configuration server and creating the required Microsoft Internet Information Services (IIS) website.
- Reading the pre-installed SSL certificate so that it can be enabled on the IIS website.
- Creating the App Orchestration configuration server machine account on the database server so that the App Orchestration configuration server can communicate with the App Orchestration database.
- Creating the App Orchestration database on the database server.

Minimum permissions

Ensure that the account you use has the following permissions.

- Membership of the local administrators group on the App Orchestration configuration server.
- Membership of the domain group which acts as the administrators group for the App Orchestration deployment.

  This administrators group must be specified when you first configure the App Orchestration configuration server and must be created before you run the Citrix App Orchestration Server Configuration wizard.

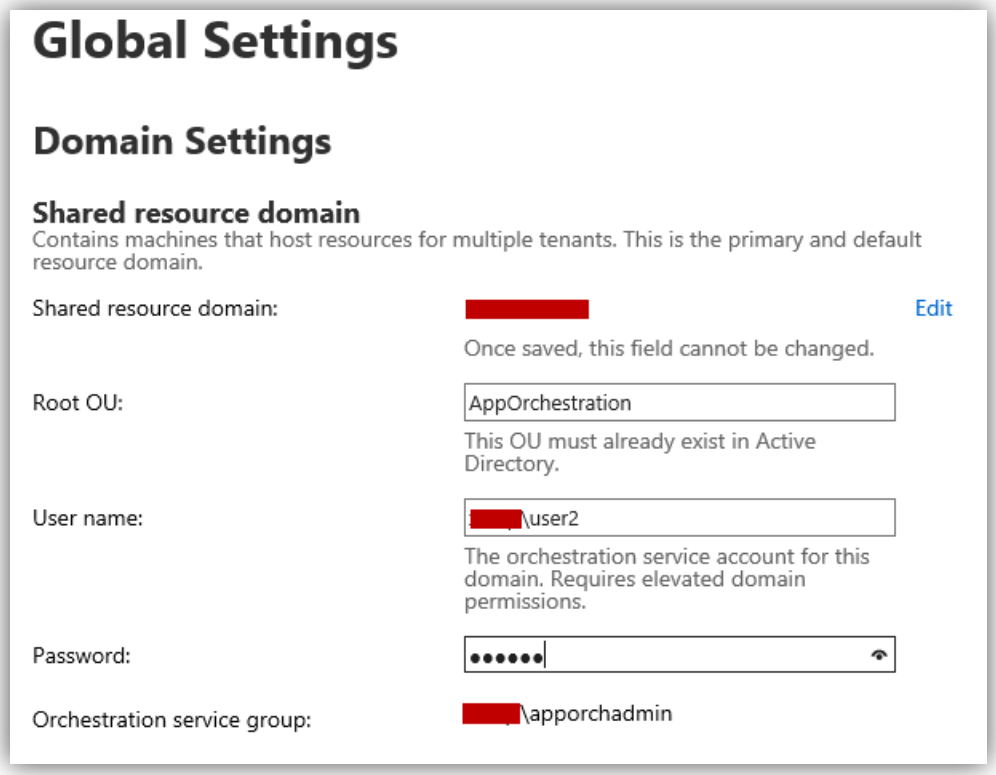


- Membership of the system administrator group on the App Orchestration database server.

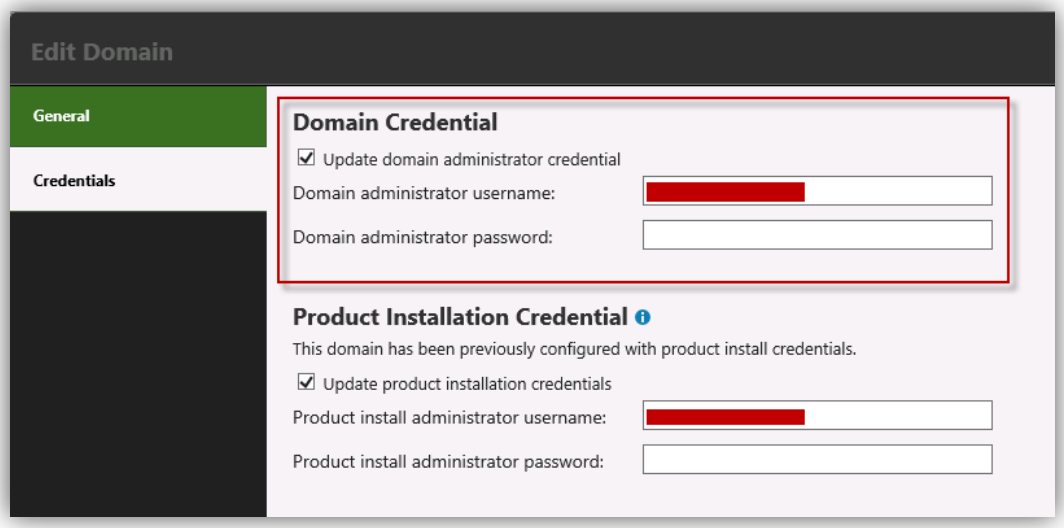
Shared resource domain credentials

Where specified

You specify this domain administrator account during initial configuration of App Orchestration.



After initial configuration, you can update the shared resource domain credentials on the **Edit Domain** screen of the App Orchestration web management console.



Actions performed using these credentials

This account is used for the following functions.

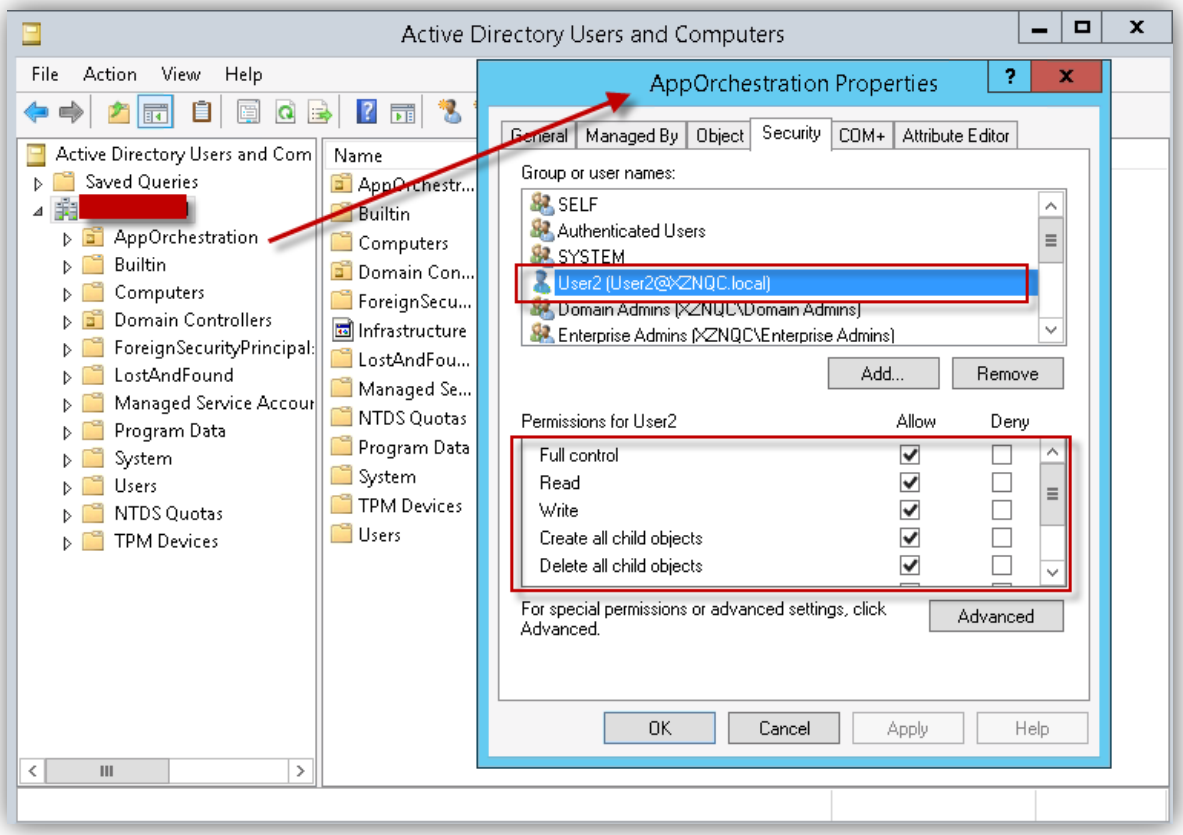
- Microsoft Active Directory organizational unit (OU) operations:
    - Verifying that the App Orchestration root OU exists.
    - Creating the DecommissionedServers OU after initial configuration of App Orchestration global settings.
    - Creating all necessary OUs during subscription creation operations.
- Machine operations:
    - Moving Delivery Controllers to the correct OU.
    - Moving Session Machines to the correct Delivery Group OU.
- User verification (if the shared user domain is the same as the shared resource domain):
    - Verifying that the specified user group exists during subscription.
    - Verifying that the specified groups are user groups and not just users.
    - Verifying that the specified user group belongs to the local user group, which is created outside of App Orchestration.
- Creating the compute resources to support integrated provisioning.
- Remotely accessing the base VM to create the integrated provisioning template.

Minimum permissions

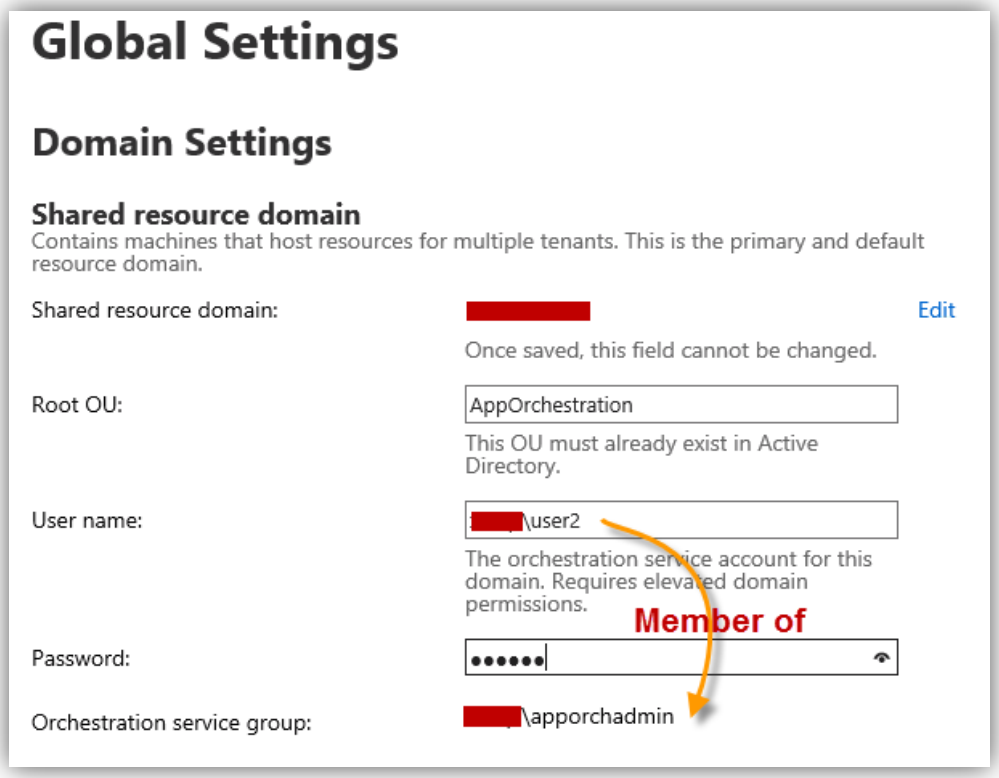
Ensure that the account you use has the following permissions.

- **Full control** permissions for the App Orchestration root OU.

  You define the root OU during initial configuration of App Orchestration and it must exist in the shared resource domain before starting initial configuration.



- Membership of the orchestration service group.



- Membership of the local administrators group on the App Orchestration configuration server.
- Membership of the local administrators group on the integrated provisioning base VM.

Shared user domain credentials

Where specified

As with the shared resource domain credentials, you specify this account during initial configuration of App Orchestration and can update the credentials on the **Edit Domain** screen of the App Orchestration web management console.

Actions performed using these credentials

This account is used for the following functions.

- Verifying that the specified user group exists during subscription.
- Verifying that the specified groups are user groups and not just users.
- Verifying that the specified user group belongs to the local user group, which is created outside of App Orchestration.

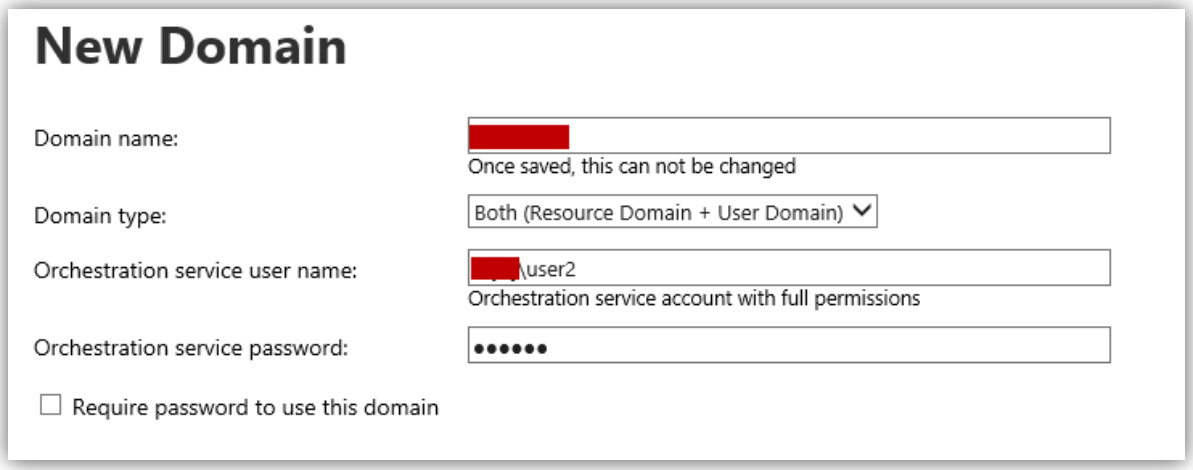
Minimum permissions

Ensure that the account you use has read permissions on the Active Directory deployment.

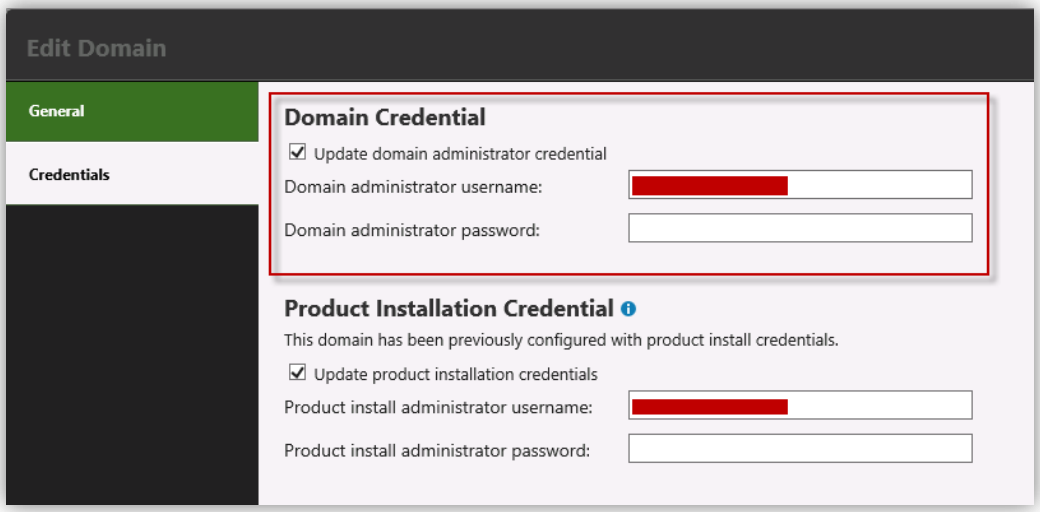
Migrated tenant resource domain credentials

Where specified

You specify these credentials when you create a new domain.



You can update the migrated tenant resource domain credentials on the **Edit Domain** screen of the App Orchestration web management console.



Actions performed using these credentials

This account is used for the following functions.

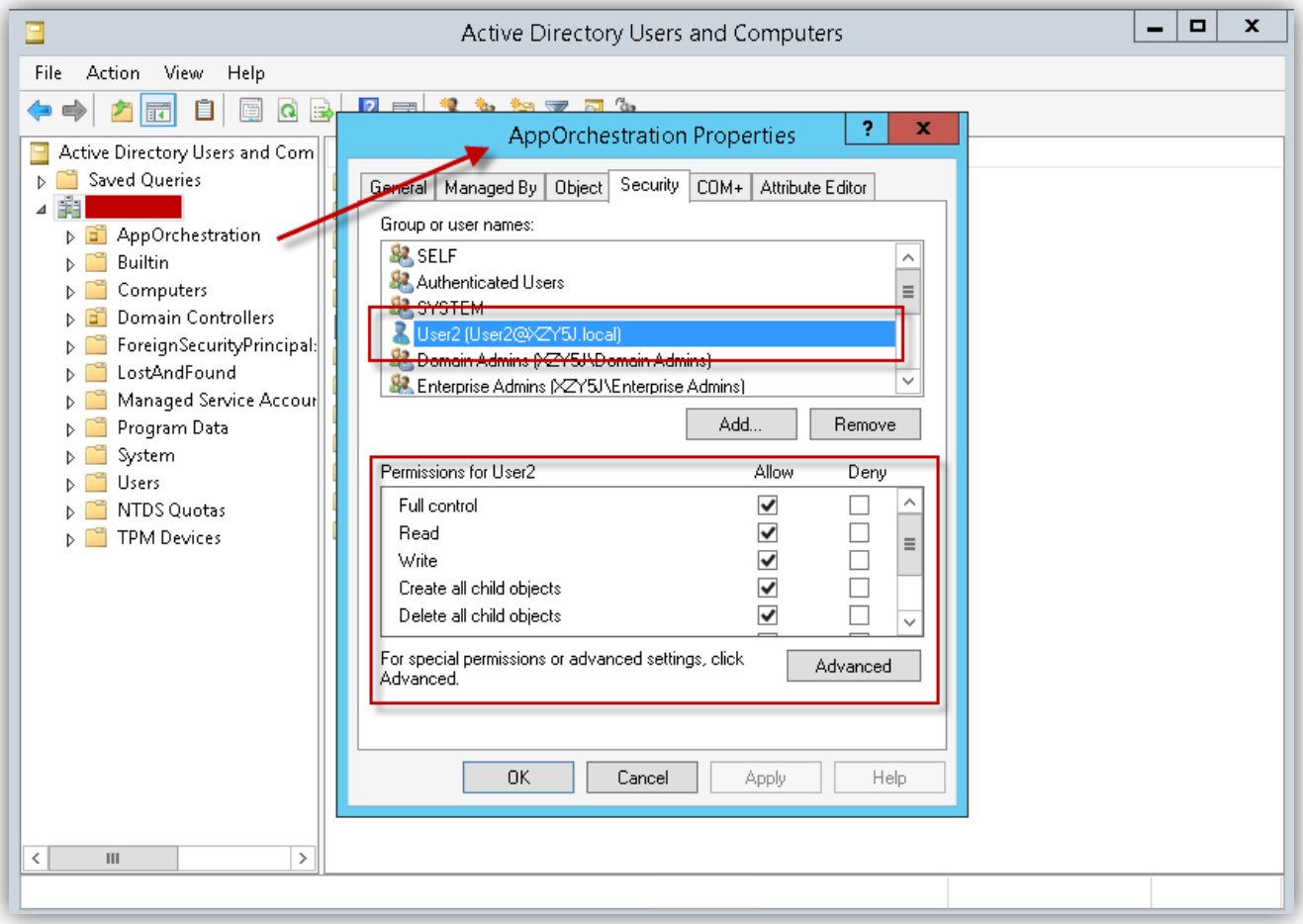
- OU operations:
  - Verifying that the App Orchestration root OU exists.
  - Creating all necessary OUs during subscription creation operations.
- Machine operations:
  - Moving Delivery Controllers to the correct OU.
  - Moving Session Machines to the correct Delivery Group OU.

- User verification (if the tenant user domain is the same as the tenant resource domain):
  - Verifying that the specified user group exists during subscription.
  - Verifying that the specified groups are user groups and not just users.
  - Verifying that the specified user group belongs to the local user group, which is created outside of App Orchestration.

Minimum permissions

Ensure that the account you use has **Full control** permissions for the App Orchestration root OU.

You must create the root OU in the tenant resource domain before you migrate the domain to the App Orchestration environment.



Migrated tenant user domain credentials

Where specified

As with the migrated tenant resource domain credentials, you specify this account when you create a new domain and can update the credentials on the **Edit Domain** screen of the App Orchestration web management console.

Actions performed using these credentials

This account is used for the following functions if the tenant user domain is the same as the tenant resource domain.

- Verifying that the specified user group exists during subscription.
- Verifying that the specified groups are user groups and not just users.
- Verifying that the specified user group belongs to the local user group, which is created outside of App Orchestration.

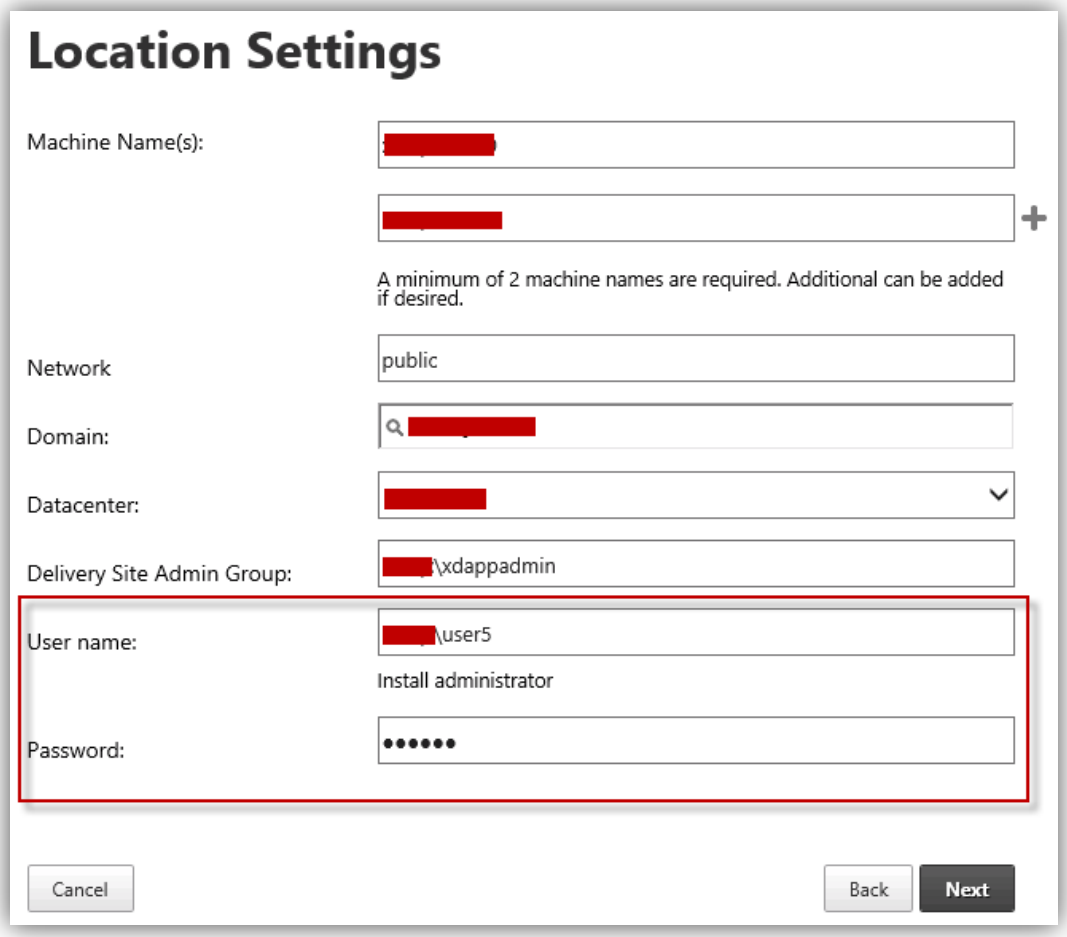
Minimum permissions

Ensure that the account you use has read permissions on the Active Directory deployment.

Delivery Site credentials for the shared resource domain

Where specified

You specify these credentials when you create a Delivery Site.



Actions performed using these credentials

This account is used for the following functions.

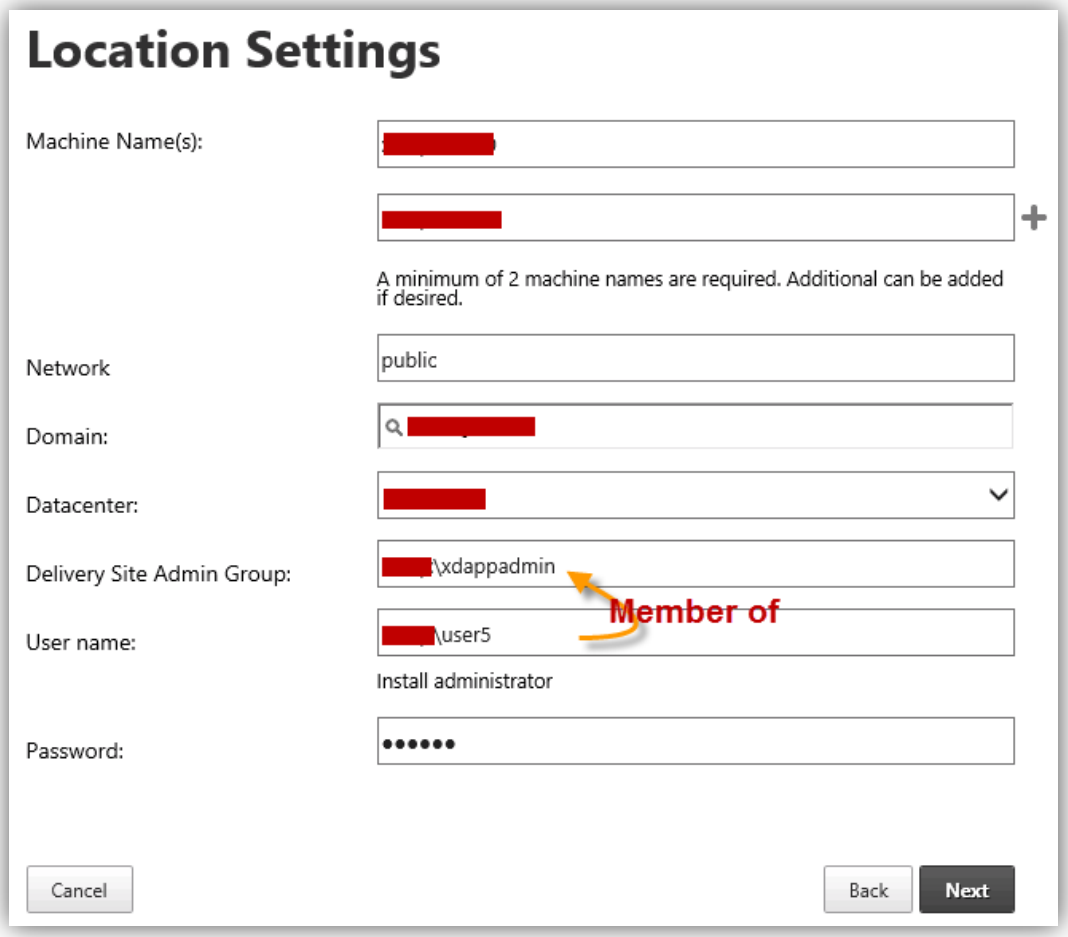
- Installing Delivery Controllers.
- Establishing a remote Windows PowerShell session from a Delivery Controller to a Session Machine in the shared resource domain or tenant resource domain so that the Session Machine can be joined to the Delivery Site.
- Verifying users when hosted applications are created.
- Establishing a remote Windows PowerShell session from a Delivery Controller to a Session Machine in the shared resource domain or tenant resource domain so that the Session Machine can be removed from the Delivery Site.
- Group Policy operations:
    - Creating the license server Group Policy Object.
    - Linking the license server Group Policy to the App Orchestration OU.
    - Creating the Delivery Controller Group Policy.
    - Linking the Delivery Controller Group Policy to a specific workload/Delivery Group OU.
- Integrated provisioning support:
    - Creating Session Machine accounts under the App Orchestration root OU in the shared resource domain and tenant resource domain.
    - Removing Session Machine accounts from the shared resource domain and tenant resource domain.
    - Moving Session Machine accounts to Delivery Group OUs in the shared resource domain and tenant resource domain.

Minimum permissions

Ensure that the account you use has the following permissions.

- **Full control** permissions for the App Orchestration root OU in the shared resource domain.
- Permission to create Group Policy Objects.
- **Full control** permissions for the App Orchestration root OU in the tenant resource domain.

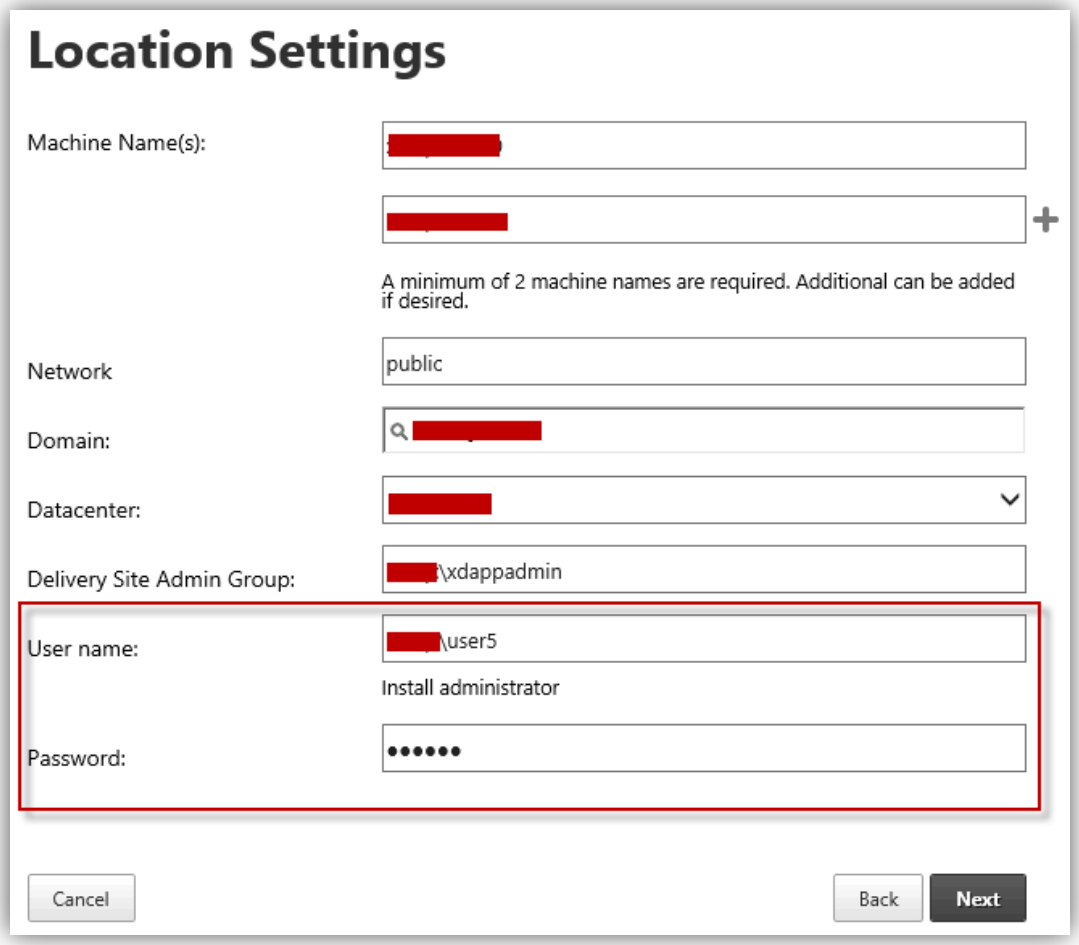
  This means that you must create a two-way trust relationship between the shared resource domain and the tenant resource domain.
- Membership of the local administrators group on all of the Desktop Controllers.
- Membership of the local administrators group on the Session Machines in the shared resource domain.
- Membership of the local administrators group on the Session Machines in all the tenant resource domains if these Session Machines need to be added to the Delivery Site in the shared resource domain, such as when creating private Delivery Group subscriptions.
- Membership of the system administrator group on all the XenDesktop database servers.
- Membership of the Delivery Site administrators group.



Delivery Site credentials for the tenant resource domain

Where specified

You specify these credentials when you migrate a Delivery Site from the tenant resource domain.



Actions performed using these credentials

This account is used for the following functions.

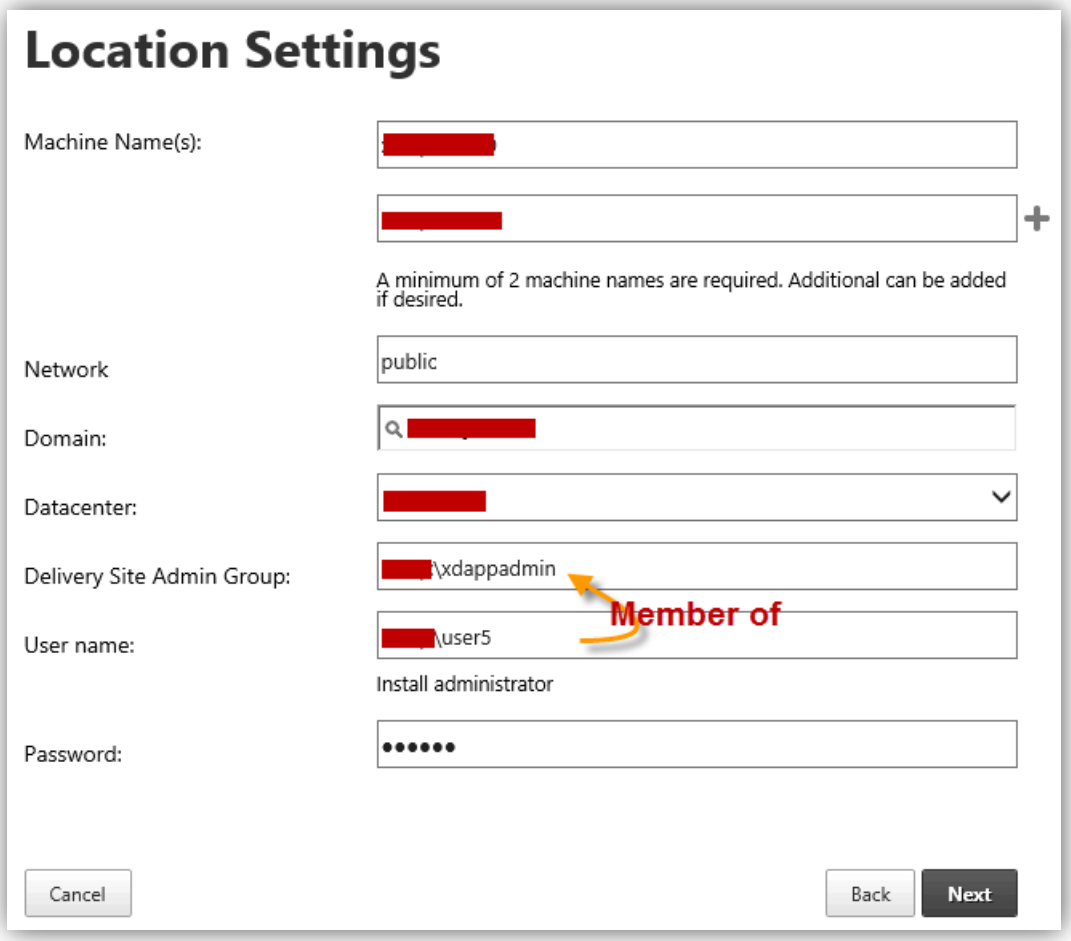
- Installing Delivery Controllers in the tenant resource domain.
- Establishing a remote Windows PowerShell session from a Delivery Controller to a Session Machine in the tenant resource domain so that the Session Machine can be joined to the Delivery Site when creating a private Delivery Site subscription or private Delivery Group.
- Verifying users when hosted applications are created.
- Establishing a remote Windows PowerShell session from a Delivery Controller to a Session Machine in the tenant resource domain so that the Session Machine can be removed from the Delivery Site.

- Group Policy operations:
    - Creating the license server Group Policy Object.
    - Linking the license server Group Policy to the App Orchestration OU.
    - Creating the Delivery Controller Group Policy.
    - Linking the Delivery Controller Group Policy to a specific workload/Delivery Group OU.

Minimum permissions

Ensure that the account you use has the following permissions.

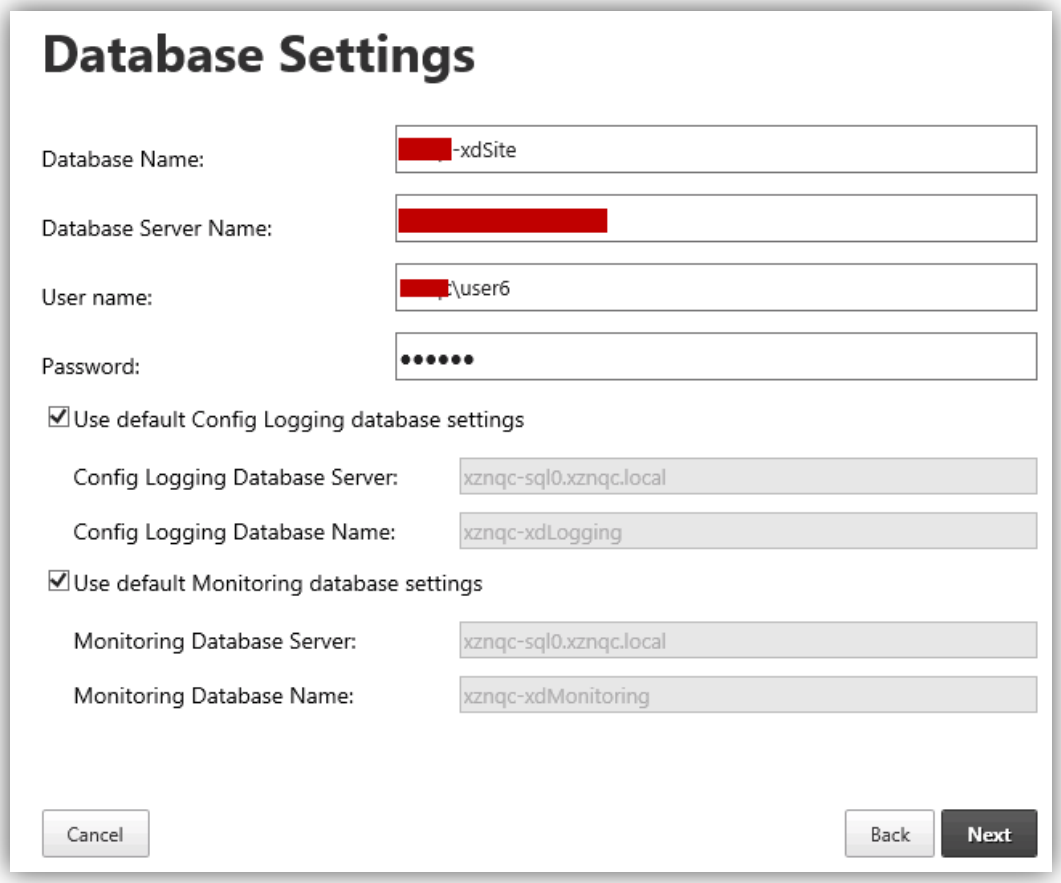
- Permission to create Group Policy Objects.
- **Full control** permissions for the App Orchestration root OU in the tenant resource domain.
- Membership of the local administrators group on all of the Desktop Controllers.
- Membership of the local administrators group on the Session Machines in all the tenant resource domains.
- Membership of the system administrator group on all the XenDesktop database servers.
- Membership of the Delivery Site administrators group.



Delivery Site database creation credentials (XenDesktop)

Where specified

You specify these credentials when you create a Delivery Site.



Actions performed using these credentials

This account is used for the following functions.

- Creating the XenDesktop database and tables.
- Creating Delivery Controller machine accounts.

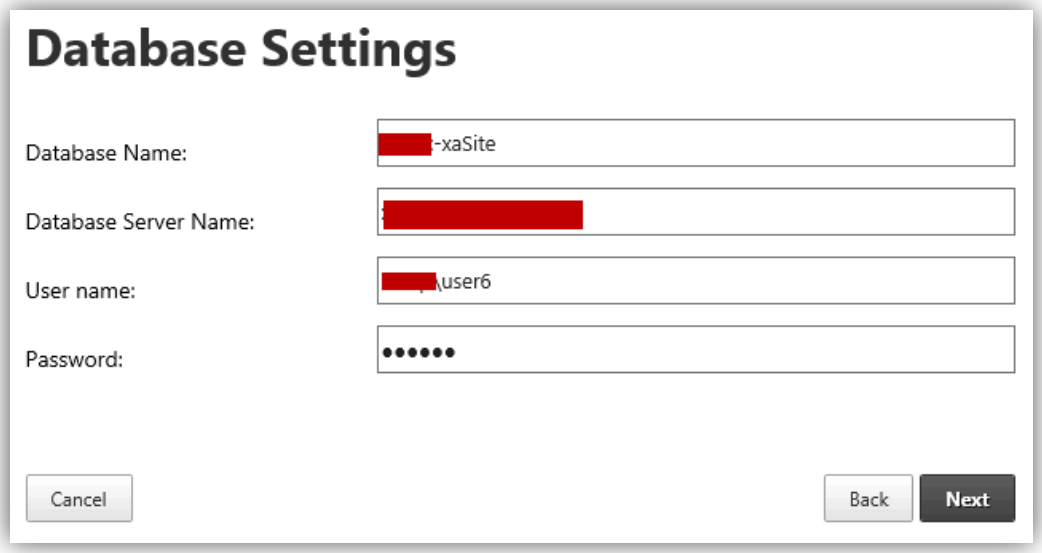
Minimum permissions

Ensure that the account you use is a member of the system administrator group on the XenDesktop database server.

Delivery Site database creation credentials (XenApp)

Where specified

You specify these credentials when you create a Delivery Site.



Actions performed using these credentials

This account is used to create the XenApp database and tables.

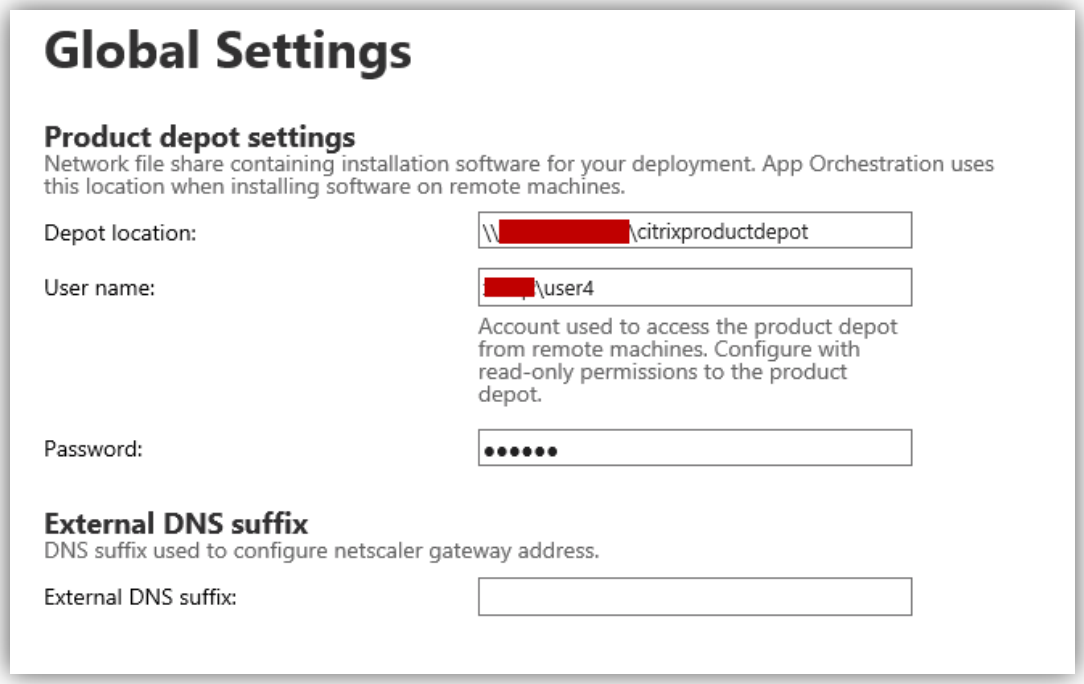
Minimum permissions

Ensure that the account you use is a member of the system administrator group on the XenApp database server.

Citrix Product Depot access credentials

Where specified

You specify this account during initial configuration of App Orchestration.



Actions performed using these credentials

This account is used to read the installation package.

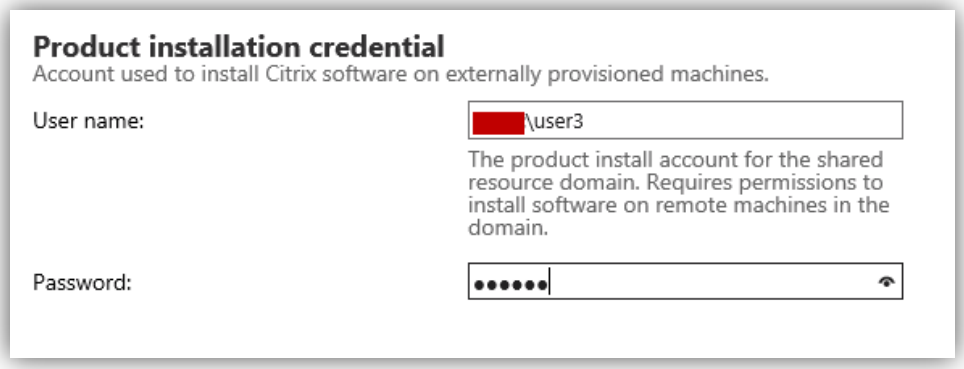
Minimum permissions

Ensure that the account you use has read permissions on the Citrix Product Depot.

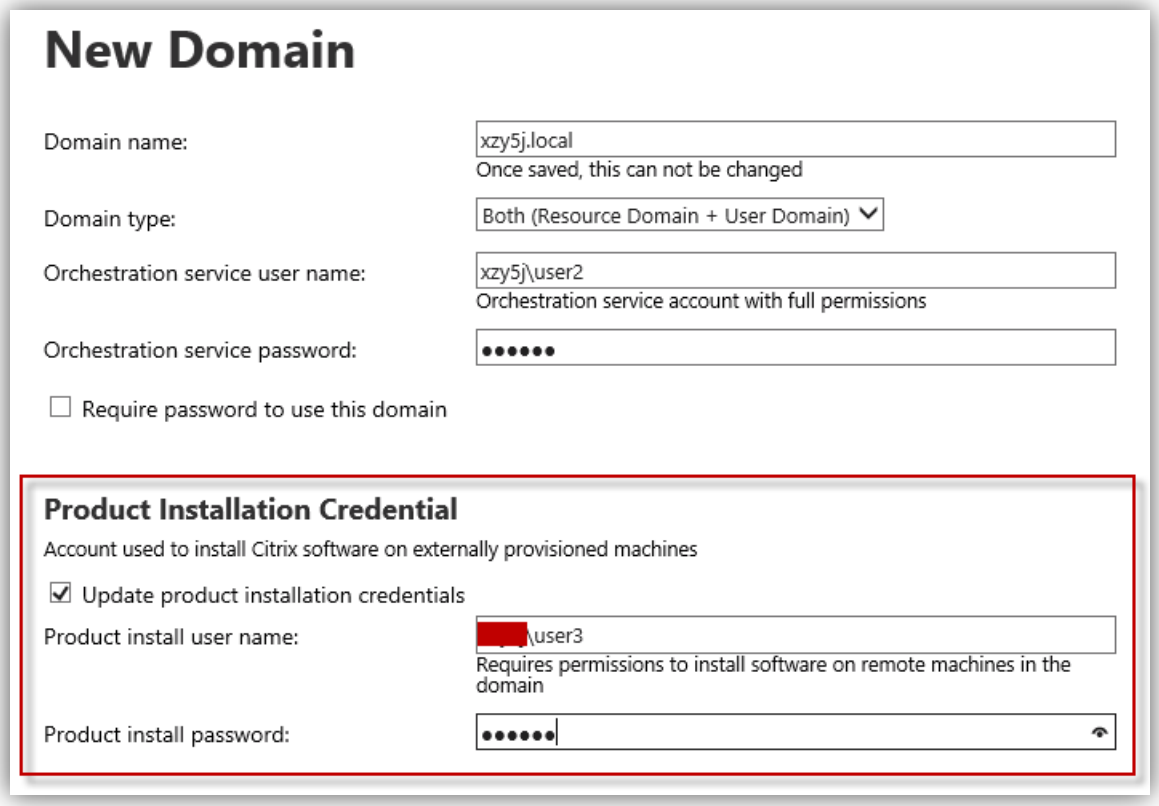
Product installation credentials

Where specified

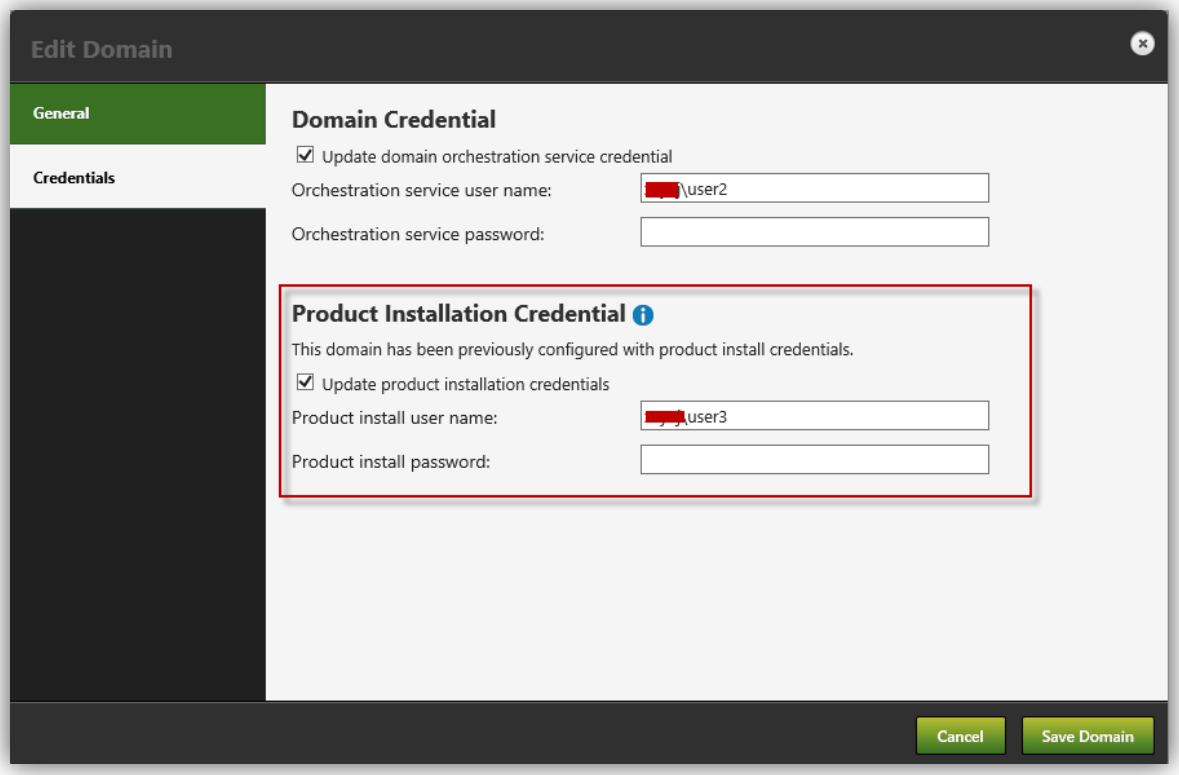
You specify this account during initial configuration of the shared resource domain.



You also enter the product installation credentials during domain migration to the tenant resource domain.



You can update these credentials on the **Edit Domain** screen of the App Orchestration web management console.



Actions performed using these credentials

This account is used for the following functions.

- Installing the Citrix App Orchestration Agent service on Delivery Controllers.
- Installing the Citrix App Orchestration Agent service on StoreFront server group machines.
- Installing XenApp on Session Machines.
- Installing the Virtual Desktop Agent and configuring Microsoft Remote Desktop Services on Session Machines.
- Installing StoreFront and configuring the StoreFront server group.
- Performing image analysis on Session Machines to determine the operating system and obtain application information.

Minimum permissions

Ensure that the account you use has the following permissions.

- Membership of the local administrators group on all of the Desktop Controllers.
- Membership of the local administrators group on all of the Session Machines.
- Membership of the local administrators group on all of the StoreFront server group machines.