



Troubleshooting Citrix- Published Resources Configuration in VMware Identity Manager

VMware Identity Manager

NOV 2018 V5

Table of Contents

Overview.....	1
Supported Versions of Components	1
Prerequisites	1
Checkpoints for Integration Broker Setup	2
Tips for a Successful Configuration	3
Log Files	4
Troubleshooting.....	4

Overview

Integrating Citrix-published resources with VMware Identity Manager™ enables you to provide VMware Workspace™ ONE™ users access to their entitled Citrix-published applications and desktops.

This document provides information about troubleshooting the configuration of Citrix-published resources in VMware Identity Manager. It includes information about required prerequisites, checkpoints that you can use for the Integration Broker setup, and common problems and solutions.

This document supplements the *Setting up Resources in VMware Identity Manager* guide, located at <https://www.vmware.com/support/pubs/identitymanager-pubs.html>.

Additional information:

- [VMware Identity Manager documentation](#)
 - “Providing Access to Citrix Published Resources” in *Setting up Resources in VMware Identity Manager*
 - “Troubleshooting VMware Identity Manager Resource Configuration” in *Setting up Resources in VMware Identity Manager*
 - Release Notes
- [VMware Identity Manager Product information](#) (click Resources)
- [Knowledge Base articles](#)
- [Support](#)

Supported Versions of Components

Verify that you are using supported versions of the various components.

- VMware Identity Manager supports Citrix XenApp 6.0, 6.5, and 7.x, XenDesktop 7.x, and Citrix Virtual Apps and Desktops 7 1808.
NOTE: Beginning with VMware Identity Manager 3.3, XenApp 5.x is no longer supported.
- To use Citrix NetScaler, Integration Broker 2.4 or later is required.
- To use XenApp or XenDesktop 7.x, Integration Broker 2.6 or later is required.
- To use the Citrix StoreFront API for application launch, Integration Broker 2.9.1 or later is required.
- Supported operating systems for the Integration Broker are Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016.
- A single Integration Broker instance can support multiple Citrix environments.

NOTE: Using the latest available version of VMware Identity Manager and its components is recommended.

Prerequisites

Verify that these prerequisites are met.

- If you are using XenApp or XenDesktop 7.x, ensure that Citrix Studio is installed on the Integration Broker server.
- Make sure the relevant Citrix SDKs are installed on the Integration Broker server to enable Citrix PowerShell Remoting.

Citrix Version	Requirement
Citrix Virtual Apps and Desktops 7 1808	Citrix Studio
XenApp or XenDesktop 7.x	Citrix Studio
XenApp 6.5	Citrix PowerShell SDK 6.5
XenApp 6.0	Citrix PowerShell SDK 6.0

Note: If the Integration Broker connects to multiple Citrix versions, install the SDKs required for all the versions.

- Verify that Microsoft Visual J# 2.0 64-bit Redistributable Package – Second Edition is installed on the Integration Broker server. This is only required if you are using the Citrix Web Interface SDK for application launch, instead of the Citrix StoreFront API.
- Verify that the Citrix Web Interface SDK is installed on the Integration Broker, unless you plan to use the Citrix StoreFront API for application launch.
- Collect the Citrix XML FQDN and port details from the Citrix Delivery Controllers. Also collect the STA server information, if applicable.
- Ensure that the XenApp server or NetScaler server is configured with user name and password authentication. VMware Identity Manager does not support other authentication methods on the XenApp server or NetScaler server such as Smart Card, HTML 5, 2 factor authentication, or SAML authentication (Citrix FAS).
- Make sure that the Active Directory users and groups entitled to Citrix-published resources have already been synchronized to VMware Identity Manager by the separate directory sync process.
- Make sure the Active Directory users and groups have been assigned to the correct Delivery Group in Citrix. If you select settings to restrict users, make sure that you specify the Active Directory users or groups.

Checkpoints for Integration Broker Setup

If the Integration Broker is not set up correctly, it can prevent the sync and launch of Citrix-published resources. Integration Broker setup issues are the most common cause of sync and launch failures.

Verify that the following settings are configured correctly in the Integration Broker server.

- Server Roles:
 - Application Server
 - File Server
 - Web IIS Support
 - IIS 6 Management Compatibility
- Verify that Microsoft Visual J# 2.0 x64-bit Redistributable Package – Second Edition is installed on the Integration Broker server (required only if you are using the Citrix Web Interface SDK).

- Verify that the required Citrix SDKs are installed.
- IIS settings:
 - Application Pool:
 - Enable 32-bit set to True
 - Identity set to a user that is a domain user, has the permissions to enable PowerShell Remoting on the Integration Broker server, and is Read-only administrator on the Citrix servers
 - NET 2.0 selected

NOTE: Ensure that these settings are configured on the application pool that is used for the Integration Broker, which may be different from the Default Application Pool.
 - HTTPS Binding
- Verify Citrix PowerShell Remoting is enabled on the Citrix XML Servers.
- Verify the setup using the Integration Broker health check REST API:
`http://localhost/IB/API/RestServiceImpl.svc/ibhealthcheck`
- Verify the setup using the XenApp Farm REST API (version 6.5):
`http://localhost/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=XenFarmServerHostname&xenappversion=Version65orLater`
- Verify the setup using the XenApp Farm REST API (version 7.x):
`http://localhost/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=XenFarmServerHostname&xenappversion=Version7x`
- If the ReST API fails for XenApp 7.x, install Citrix Studio if it is not already installed, and try again.

Tips for a Successful Configuration

Use the following tips to avoid common problems.

- Certificates are not required for proof-of-concept environments but strongly recommended for production environments.

 VMware Identity Manager does not rotate certificates. Plan your strategy for certificate refreshes accordingly.
- In XenDesktop and XenApp 7.9, published applications are assigned to users differently than in earlier versions. In earlier versions, you specified an Active Directory group or user account to gain access to a Citrix resource. Since version 7.9, all authenticated users have access to all applications by default. To restrict users, a new option, Limited Visibility Group, can be used. You add users or groups to the Limited Visibility Group, and only those users will be able to see the applications.

 Ensure that if the Limited Visibility Group option is selected, it contains users or groups. If it does not contain any users or groups, sync to VMware Identity Manager will not work.
- In XenApp 6.x, you can publish an RDSH Desktop. When users launch a XenApp 6.x published desktop in VMware Identity Manager, they will not see the Citrix connection bar at the top of the screen. If users are expecting to see this bar (based on how it is configured in Citrix), you can change the configuration in VMware Identity Manager to force the bar to be shown.
 1. Log in to the VMware Identity Manager console as an admin user.

2. Click the arrow on the **Catalog** tab and select **Settings**.
3. Select **Citrix Published Application > ICA Configuration**.
4. Enter `Connectionbar=1` in the ICA Launch Properties text box, then click **Save**.
5. Launch the application again.

Log Files

View the following log files to troubleshoot problems with the Citrix-published resources configuration:

- Integration Broker log: `%programdata%/VMware/HorizonIntegrationBroker`

Troubleshooting

Use this information to troubleshoot problems with the sync and launch of Citrix-published resources in VMware Identity Manager.

Viewing Launch Errors in the Dashboard

You can troubleshoot Horizon, Horizon Cloud, and Citrix resource launch failures by viewing error messages about the root cause and suggested solutions in the VMware Identity Manager console.

1. In the VMware Identity Manager console, select the **Dashboard > Reports** tab.
2. Select **Audit Events** from the list of reports.
3. Set the **Type** as **LAUNCH** or **LAUNCH_ERROR**.
4. Select a time frame and click **Show**.

Launch of Citrix-published Resources Fails if XML Port is Set Incorrectly

Problem: Launch of Citrix-published resources from a Citrix 7.x or 6.x server farm fails if the XML Port is set incorrectly in VMware Identity Manager.

Solution: Ensure that the XML port is set correctly.

In a XenApp 6.x or earlier environment, ask the Citrix administrator to run `CTXXMLS.EXE` to verify the port or browse to the following location within the registry on the XenApp Management server:

```
HKLM/SYSTEM/CurrentControlSet/Services/CtxHttp | TcpPort=
```

Verify the port number. By default the port is set to 80, but it is commonly changed to 8080 or 88. Ensure that the correct port is set in the VMware Identity Manager Citrix configuration in the **Catalog > Manage Desktop Applications > Citrix Published Application** page.

For XenDesktop 7.x, see <https://support.citrix.com/article/CTX127945> for information on verifying the XML port. Ensure that the correct port is set in the VMware Identity Manager Citrix configuration, in the **Catalog > Manage Desktop Applications > Citrix Published Application** page.

Citrix Resource Sync Fails if Limited Visibility Group Does Not Contain Any Users or Groups

Problem: In XenDesktop and XenApp 7.9 and later, if the Limited Visibility Group setting is selected and if it does not contain any users or groups, sync to VMware Identity Manager fails.

Solution: If set, the Limited Visibility Group must contain users or groups.

1. Find the actual name of the application by running the following PowerShell commands:

```
asnp citrix*
Get-brokerapplication-browsername nameofCitrixPublishedResource
```
2. In the application detail that displays, look for the name of the application.
3. In Citrix Studio, find the application with that name, edit the Limited Visibility property, and add users and groups to the list.

Sync Issues if Published Applications or Desktops in a Site Do Not Contain Valid Users

Problem: All Citrix-published applications and desktops in a Site must contain valid users. If a user or group is deleted and that user or group is not removed from a Citrix-published resource, the Citrix application or desktop shows an orphaned SID. This stops the sync to VMware Identity Manager from working.

You can use the following API to check the issue:

```
http://CitrixBrokerFQDN:80/IB/API/RestServiceImpl.svc/hznxenapp/admin/entitlements?computerName=IBFQDN&xenappversion=VersionNumber&appName=applicationName
```

The resulting file contains empty resources. Example output:

```
"[{"IncludedUsers\":"DomainName\\\\"USERNAME:User$$-1-5-21-1097426297-1557994628-1672037986-53944:Group\"}]"
```

Solution: Ensure that all Citrix-published applications and desktops within a Site contain valid users.

Entitlements do not Appear in VMware Identity Manager

Problem: Entitlements to an application or delivery group are set on the Citrix server but they do not appear in VMware Identity Manager.

Solution: Ensure that the users and groups are synced to VMware Identity Manager.

1. Log in to the Citrix Management Console and locate the application that does not have any entitlements.
2. Make a note of the Active Directory users and groups that have permissions to launch the application in the Citrix Management Console.
3. Log in to the VMware Identity Manager administration console, click the **Users & Groups** tab, and verify that the users and groups appear in the list.
You can also use the search box in the top right of the page.
4. If the users and groups appear, sync Citrix resources again from the **Catalog > Manage Desktop Application > Citrix Published Application** page.
Note: The users and groups must exist in VMware Identity Manager before you sync Citrix resources. If they do not exist, the sync will run but the entitlements will not be updated.
5. If the users and groups do not exist in VMware Identity Manager:
 - a. Check where the users and groups exist in Active Directory (using Active Directory Users and Computers Snappin).
 - b. In the VMware Identity Manager administration console, update the AD Sync DN's for the users and groups in the directory's **Sync Settings** pages.
 - c. When the users and groups appear in the VMware Identity Manager administration console, sync Citrix resources again.

When sync completes, the entitlements appear in VMware Identity Manager.

Exception During Sync if Application Pool Identity is not Configured

Problem: An exception occurs during the sync of Citrix resources to VMware Identity Manager because of a common error in the Integration Broker setup, where the Identity setting has been configured for the wrong application pool.

During sync, the following exception occurs in the Integration Broker log:

```
IntegrationBrokerLogger Error 1002 2017-04-04 19:10:38,936 (16)
HznXenIntegrationBroker.ApplicationExceptionHandler - Connecting
to remote server failed with the following error message: The client cannot
connect to the destination specified in the request. Verify that the service on
the destination is running and is accepting requests. Consult the logs and
documentation for the WS-Management service running on the destination, most
commonly IIS or WinRM. If the destination is the WinRM service, run the
following command on the destination to analyze and configure the WinRM
service: "winrm quickconfig". For more information, see the
about_Remote_Troubleshooting Help topic at
System.Management.Automation.Runspaces.AsyncResult.EndInvoke().
```

Solution: Configure the Identity setting for the application pool to which the Integration Broker is attached. This may be different from the Default Application Pool.

To verify the correct application pool:

1. In IIS Manager, click **Application Pools** in the left pane.
2. Right-click the application pool and select **View Applications**.
3. Verify that the Integration Broker appears in the list of applications.

To configure the Identity setting for the application pool, follow the instructions in *Setting up Resources for VMware Identity Manager*.

ICA File is Not Created During Citrix Resource Launch

Problem: When users try to launch a Citrix resource, the ICA file is not created and the following exception appears in the Integration Broker log:

```
IntegrationBrokerLogger Information 1004 2017-05-02 11:50:42,093 (8)
HznXenIntegrationBroker.API.RestServiceImpl - Get ICA file contents for
AppNameCitrix.MPS.App.XA65Test.Airwatch Notepad Test, Farm Name: XA65Test,
Server Name:serverName, Username: user1 IntegrationBrokerLogger Error 1002
2017-05-02 11:50:42,093 (8)
HznXenIntegrationBroker.ApplicationExceptionHandler - WebPNBuilder
implementation class WebPNImpl!com.citrix.wing.webpnimpl.WebPNBuilderImpl not
found at com.citrix.wing.webpn.WebPNBuilder.getInstance() at
HznXenIntegrationBroker.XenAppSDK.Impl.XenAppSDKClient.CreateUserContext(UserPr
incipal userPrincipal, String appName, Configuration configuration) at
HznXenIntegrationBroker.XenAppSDK.Impl.XenAppSDKClient.GenerateICAFileCommon(Us
erPrincipal userPrincipal, String appName, Configuration configuration) at
HznXenIntegrationBroker.XenAppSDK.Impl.XenAppSDKClient.GenerateICAFile(UserPrin
cipal userPrincipal, String farmName, String serverName, String serverPort,
String appName, XMLServiceTransportProtocol xmlserviceTransportProtocol, Int32
sslRelayPort)
```

Solution: Re-install Microsoft Visual J# 2.0 in the Integration Broker server.

Restarting Integration Broker

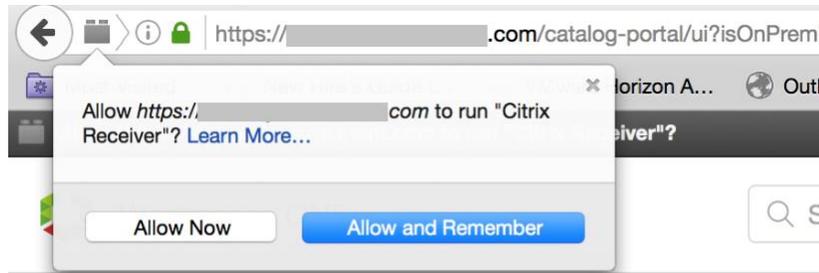
If the Integration Broker fails to respond, restart IIS.

1. Open the Command Prompt window as administrator.
2. Type `iisreset`.

Application Launch on Firefox Requires Users to Allow Citrix Receiver Plugin

On Firefox, when users launch a Citrix-published application, they are prompted to allow the Citrix Receiver plugin:

Allow `https://IdentityManagerHostname` to run Citrix Receiver?



Users must click **Allow Now** or **Allow and Remember** to launch the application.

Disabling Feature Flag for Citrix Application Launch on Chrome

Problem: Users are unable to launch Citrix applications or desktops with the Chrome browser.

Description: Citrix uses NPAPI plugins to launch applications and desktops. However, NPAPI plugin support was disabled in Chrome version 42 and later. The feature flag `orgUseNonNPAPIForCitrixLaunch` was added to VMware Identity Manager to match the Citrix application launch behavior on Citrix Storefront. If the feature flag is disabled, the browser downloads the ICA file and when the user clicks it, Citrix Receiver launches the application or desktop. If the feature flag is enabled, the browser launches the Citrix application or desktop directly on Citrix Receiver using the "RECEIVER" protocol. By default, the feature flag is enabled.

Solution: Disable the feature flag if users are unable to launch applications or desktops on Chrome. After you disable the feature flag, the browser will download the ICA file and users can click it to launch their application or desktop.

To disable the feature flag,

1. Use the following REST API:

```
PUT https://fqdn/SAAS/jersey/manager/api/tenants/settings?tenantId=tenantname
{
  "items": [
    {"name": "orgUseNonNPAPIForCitrixLaunch", "value": "false"}
  ]
}
```

with the following two headers:

```
Content-Type application/vnd.vmware.horizon.manager.tenants.tenant.config.list+json
Authorization HZN value_of_HZN_cookie_for_admin_user
```

2. Either wait 24 hours for the change to take effect or restart the VMware Identity Manager service.

To restart the service on Linux, log in to the virtual appliance and run the following command:
`service horizon-workspace restart`

To restart the service on Windows, run the following script:

```
install_dir\usr\local\horizon\scripts\horizonService.bat restart
```

Entitlements are Not Synced to VMware Identity Manager or Some Entitlements are Missing

If Citrix entitlements are not synced to VMware Identity Manager or some entitlements are missing, follow these steps to troubleshoot the entitlements sync:

1. Call the following ReST API:

- For a Citrix server farm 7.x application:
`http://IntegrationBrokerServerFQDN/IB/API/RestServiceImpl.svc/hznxenapp/admin/entitlements?domainName&username&password&computerName=XenFarmServerName&appName=applicationName&xenappversion=Version7x`
- For a Citrix server farm 7.x delivery group:
`http://IntegrationBrokerServerFQDN/IB/API/RestServiceImpl.svc/hznxenapp/admin/deliveryGroup/entitlements?domainName&username&password&computerName=XenFarmServerName&deliveryGroupName=deliveryGroupName&xenappversion=Version7x`
- For a Citrix server farm 6.5 application:
`http://IntegrationBrokerServerFQDN/IB/API/RestServiceImpl.svc/hznxenapp/admin/entitlements?domainName&username&password&computerName=XenFarmServerName&appName=applicationName&xenappversion=Version65orLater`

For example, if you are troubleshooting entitlements for the NotePad application on a Citrix 7.x server farm, use:

```
http://IntegrationBrokerServerFQDN/IB/API/RestServiceImpl.svc/hznxenapp/admin/entitlements?domainName&username&password&computerName=XenFarmServerName&appName=notepad&xenappversion=Version7x
```

2. Check whether the entitlements in the API response match the entitlements on the Citrix server.
3. Check whether those users and groups are synced to VMware Identity Manager. In the administration console, click the **Users & Groups** tab to view users and groups.
4. If the users and groups are not synced to VMware Identity Manager, first perform a directory sync and then manually sync the Citrix virtual apps collection.

Additional Troubleshooting Information

For additional troubleshooting topics, see the “Troubleshooting VMware Identity Manager Resource Configuration” section in *Setting up Resources in VMware Identity Manager*.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.