University of Roehampton London

# Patch Management Policy

| | |
|---|---|
| Owner: | |
| Approver (Date): | |
| Review due date: | September 2020 |
| Current Version: | 1.1 |
| Update history: | 22/01/2019 Document Creation<br>20/03/2020 Minor amendments to bring into line with Cyber Essentials |
| Document Type: | Operational Policy |
| Classification: | Internal Only |

To discuss receiving the document in an alternative format, please contact University Secretariat.

## Contents

## 1. Introduction

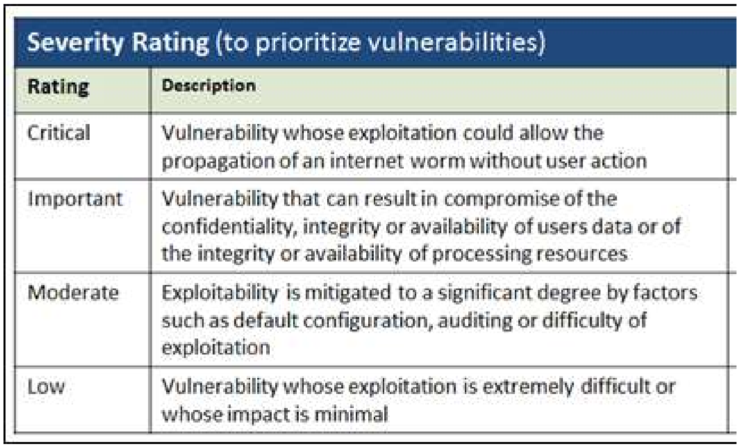
1.1 This document describes the requirements for maintaining up-to-date systems and software on all IT Systems managed or maintained by the University of Roehampton.

1.2 The University of Roehampton has a responsibility to uphold the confidentiality, integrity and availability of the data held on its IT systems on and off site which includes systems and services supplied by third parties but managed by the University of Roehampton.

1.3 The University has an obligation to provide appropriate and adequate protection of all its IT estate whether physical, virtual, on premise or in the Cloud.

1.4 Effective implementation of this policy reduces the likelihood of system compromise due to known vulnerabilities

1.5 Patches are rated as shown in the tables below.



Severity Rating (to prioritize vulnerabilities)

| Rating | Description |
|---|---|
| Critical | Vulnerability whose exploitation could allow the propagation of an internet worm without user action |
| Important | Vulnerability that can result in compromise of the confidentiality, integrity or availability of users data or of the integrity or availability of processing resources |
| Moderate | Exploitability is mitigated to a significant degree by factors such as default configuration, auditing or difficulty of exploitation |
| Low | Vulnerability whose exploitation is extremely difficult or whose impact is minimal |

Microsoft severity rating system

## 2. Scope

2.1 All IT systems owned by the University of Roehampton and managed by the University IT department.

2.2 All IT systems used by the University of Roehampton but managed by third parties.

## 3. Responsibilities

3.1 The Chief Information Officer is accountable for ensuring that the software update and patching policy is adhered to.

3.2 The IT Services Manager is responsible for ensuring that in scope software is maintained through regular software updates and patching.

3.3 System owners are responsible for ensuring that all in scope software they manage is maintained through regular software updates and patching.

3.4 The University's IT department is responsible for ensuring that all in scope software they manage is maintained through regular software updates and patching.

3.5 The University's IT department is responsible for routinely assessing compliance with the patching policy and will provide guidance to all the stakeholder groups in relation to issues of security and patch management.

3.6 Third Party Suppliers are responsible for ensuring that all in scope software they manage is maintained through regular software updates and patching, both before and during their operational deployment. Where this is not possible, this must be escalated to the Roehampton IT department.

## 4. Definitions

4.1 System Owners includes Business Systems Managers, Assistant Systems Support Analysts and Business Systems Support Analysts.

4.2 The University's IT department includes the Core Systems Manager, Solutions Analyst, Deputy Director IT and IT Security Manager.

4.3 IT Systems refers to:

- Physical Servers
- Virtual Servers
- Cloud hosted Servers
- Third Party Managed Servers
- End user compute devices (laptops/desktops etc.)
- Mobile devices (phones, tablets etc.)
- Server Operating Systems (both Microsoft and non-Microsoft)
- Server Applications – (i.e.: Microsoft IIS or SQL etc.)

- EUC Applications – (i.e.: Productivity Tools such as MS Office, Adobe Reader, and Web Browsers etc.)
- Device Firmware

## 5. Software updates and patching

5.1 All IT systems (as defined in section 4), either owned by the University of Roehampton or those in the process of being developed and supported by third parties, must be licenced appropriately , supported by the manufacturer and be running up-to-date and patched Operating systems and application software.

5.2 Any IT system that is no longer licenced or supported by the manufacturer will be removed from the University of Roehampton network.

5.3 To protect the University's IT systems from known vulnerabilities, security patches must be deployed in a suitable time frame. Unless prevented by University IT Procedures, patches should be deployed as per the following schedule:

| **Vendor vulnerability classification** | **Full deployment within (calendar days)** |
|---|---|
| Critical | 14 |
| High | 14 |
| Medium | 21 |
| Low | 28 |

5.4 Where the deployment of 'Critical' or 'High risk' security patches within 14 days is not possible, either appropriate compensating controls or a temporary means of mitigation must be applied to reduce the exposure faced by the University's IT systems.

5.5 Third party suppliers must be prepared to provide evidence of up-to-date patching before IT systems are accepted into operational service.

5.6 New systems must be patched to the current agreed baseline before coming online in order to limit the introduction of new threats.

5.7 Servers must comply with the recommended minimum requirements that are specified by the University of Roehampton's IT department which includes the default operating system level; service packs; hotfixes and patching levels. All exceptions shall be documented by the University of Roehampton's IT department.

5.8 Microsoft patches are scheduled to deploy the first Monday after "Patch Tuesday". This is the unofficial name used to refer to the day Microsoft releases its security patches which typically occurs on the second Tuesday of each month.

5.9 Servers managed by the University of Roehampton's IT department will apply regular patches according to the IT department's defined schedule:

5.10 Patches for key business systems, such Finance and the Student records systems are patched manually in a controlled manner.

5.11 All patches must be tested prior to full implementation since patches may result in unforeseen issues.

5.12 Testing will be carried out using a Test system that closely matches the production systems. Where there is no Test system then patch results from another non-key production system will be used and the results of any patch will be closely monitored for adverse effects.

5.13 User Acceptance Testing (UAT) of the business system must be completed after controlled patching completes.

5.14 A remediation plan that allows for the return to a working state must be in place prior to any patching. This could be either rolling back to a last known good state or fixing forward (e.g.: removing patches from the system and/or restoration of previous backup from Microsoft DPM or Azure Backup Service or deploying a more recent hotfix to correct a problem introduced by a patch).

5.15 Systems that are removed from the network as a result of insufficient patching will only be reconnected when it can be demonstrated that they have been brought up to date and are no longer present a risk to the University of Roehampton’s network.

5.16 Those with patching roles as detailed in section 3 are required to compile and maintain reporting metrics that summarise the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk.

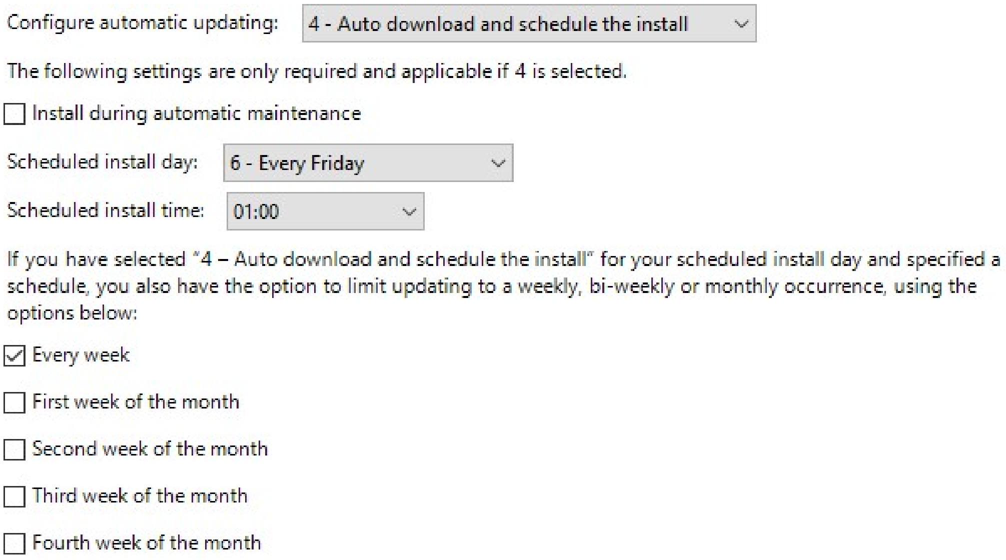
5.17 Roehampton IT will endeavour to achieve 100% compliance for patching Operating Systems under its management.

5.18 Exceptions to the patch management policy require formal documented approval from the Deputy Director of IT.

5.19 This policy is subject to review every 6 months to ensure that it is accurate, effective and up to date.

## 6. Appendix 1 – Microsoft update configuration settings

On Premises GPO controlled University of Roehampton managed Servers:



Configure automatic updating: 4 - Auto download and schedule the install

The following settings are only required and applicable if 4 is selected.

☐ Install during automatic maintenance

Scheduled install day: 6 - Every Friday

Scheduled install time: 01:00

If you have selected “4 – Auto download and schedule the install” for your scheduled install day and specified a schedule, you also have the option to limit updating to a weekly, bi-weekly or monthly occurrence, using the options below:

☑ Every week

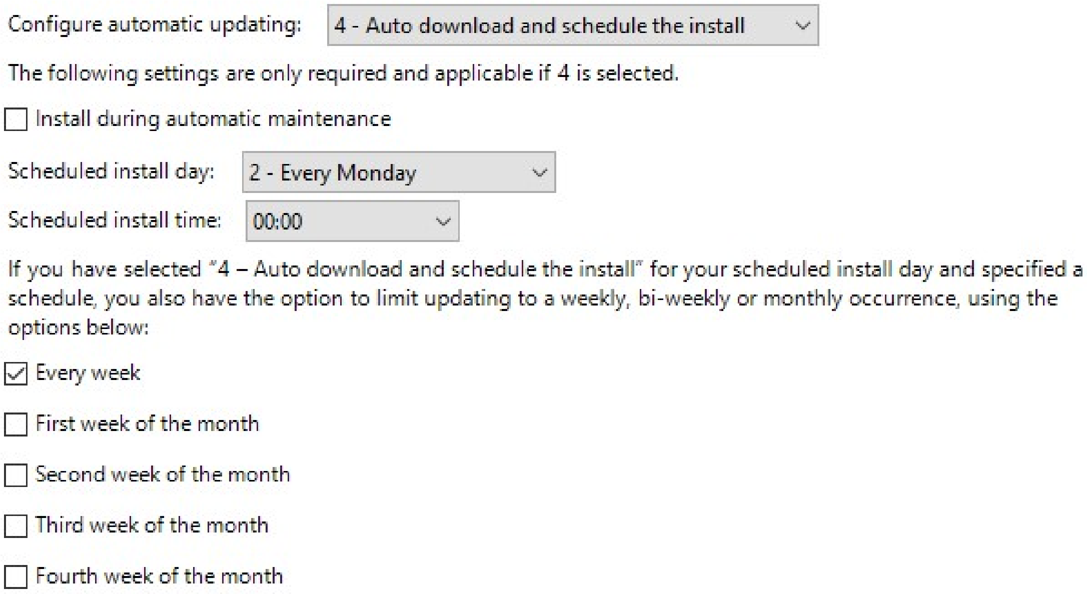
☐ First week of the month

☐ Second week of the month

☐ Third week of the month

☐ Fourth week of the month

--



Configure automatic updating: 4 - Auto download and schedule the install

The following settings are only required and applicable if 4 is selected.

☐ Install during automatic maintenance

Scheduled install day: 2 - Every Monday

Scheduled install time: 00:00

If you have selected “4 – Auto download and schedule the install” for your scheduled install day and specified a schedule, you also have the option to limit updating to a weekly, bi-weekly or monthly occurrence, using the options below:

☑ Every week

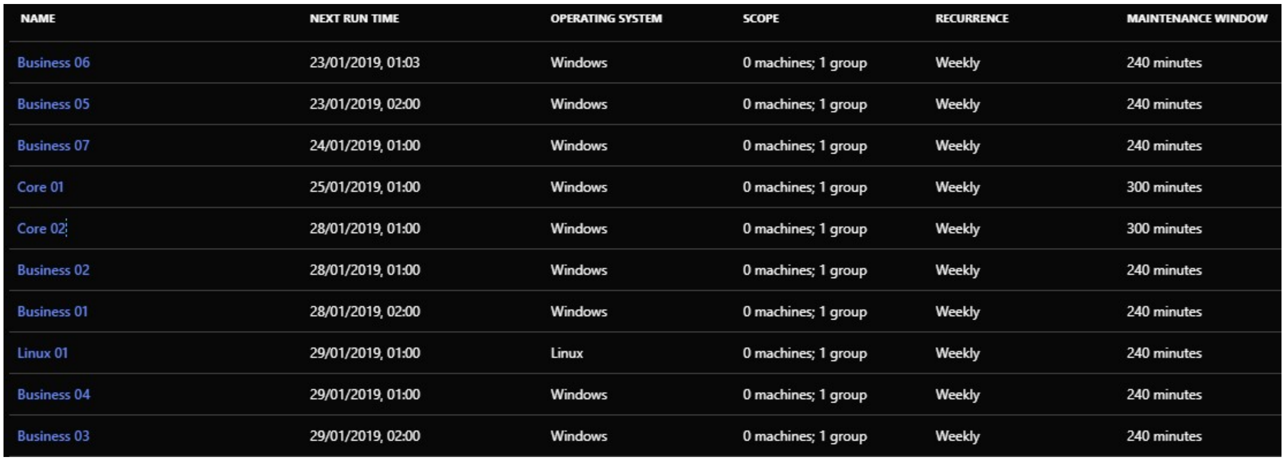
☐ First week of the month

☐ Second week of the month

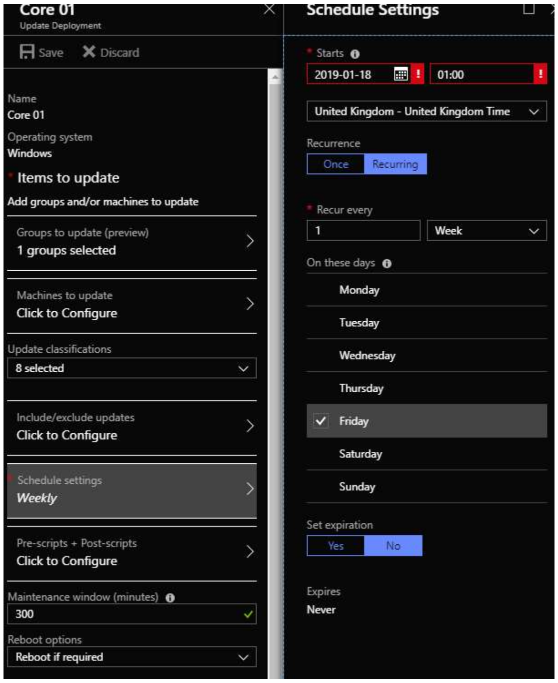
☐ Third week of the month

☐ Fourth week of the month

Cloud (Azure Update Management) University of Roehampton managed Servers:



| NAME | NEXT RUN TIME | OPERATING SYSTEM | SCOPE | RECURRENCE | MAINTENANCE WINDOW |
|---|---|---|---|---|---|
| Business 06 | 23/01/2019, 01:03 | Windows | 0 machines; 1 group | Weekly | 240 minutes |
| Business 05 | 23/01/2019, 02:00 | Windows | 0 machines; 1 group | Weekly | 240 minutes |
| Business 07 | 24/01/2019, 01:00 | Windows | 0 machines; 1 group | Weekly | 240 minutes |
| Core 01 | 25/01/2019, 01:00 | Windows | 0 machines; 1 group | Weekly | 300 minutes |
| Core 02 | 28/01/2019, 01:00 | Windows | 0 machines; 1 group | Weekly | 300 minutes |
| Business 02 | 28/01/2019, 01:00 | Windows | 0 machines; 1 group | Weekly | 240 minutes |
| Business 01 | 28/01/2019, 02:00 | Windows | 0 machines; 1 group | Weekly | 240 minutes |
| Linux 01 | 29/01/2019, 01:00 | Linux | 0 machines; 1 group | Weekly | 240 minutes |
| Business 04 | 29/01/2019, 01:00 | Windows | 0 machines; 1 group | Weekly | 240 minutes |
| Business 03 | 29/01/2019, 02:00 | Windows | 0 machines; 1 group | Weekly | 240 minutes |



Core 01
Update Deployment

Name
Core 01

Operating system
Windows

* Items to update
Add groups and/or machines to update

Groups to update (preview)
1 groups selected

Machines to update
Click to Configure

Update classifications
8 selected

Include/exclude updates
Click to Configure

Schedule settings
*Weekly*

Pre-scripts + Post-scripts
Click to Configure

Maintenance window (minutes)
300

Reboot options
Reboot if required

Schedule Settings

* Starts
2019-01-18 01:00

United Kingdom - United Kingdom Time

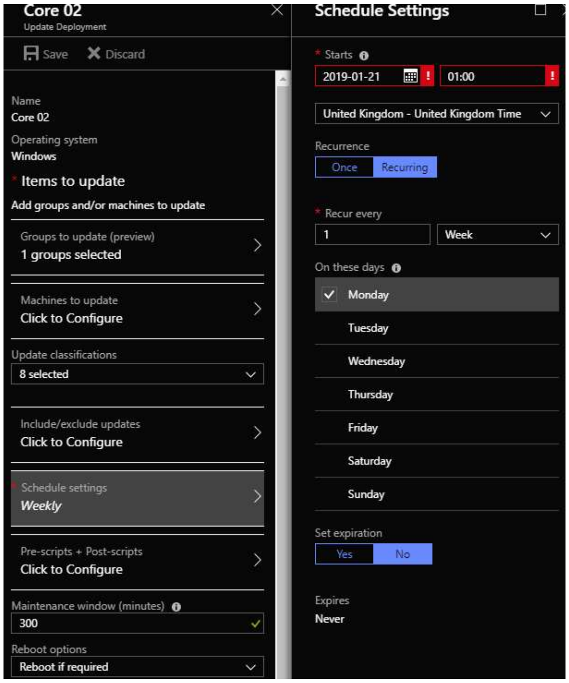
Recurrence
Once [✓ Recurring]

* Recur every
1 Week

On these days
Monday
Tuesday
Wednesday
Thursday
✓ Friday
Saturday
Sunday

Set expiration
Yes [✓ No]

Expires
Never



Core 02
Update Deployment

Name
Core 02

Operating system
Windows

* Items to update
Add groups and/or machines to update

Groups to update (preview)
1 groups selected

Machines to update
Click to Configure

Update classifications
8 selected

Include/exclude updates
Click to Configure

Schedule settings
*Weekly*

Pre-scripts + Post-scripts
Click to Configure

Maintenance window (minutes)
300

Reboot options
Reboot if required

Schedule Settings

* Starts
2019-01-21 01:00

United Kingdom - United Kingdom Time

Recurrence
Once [✓ Recurring]

* Recur every
1 Week

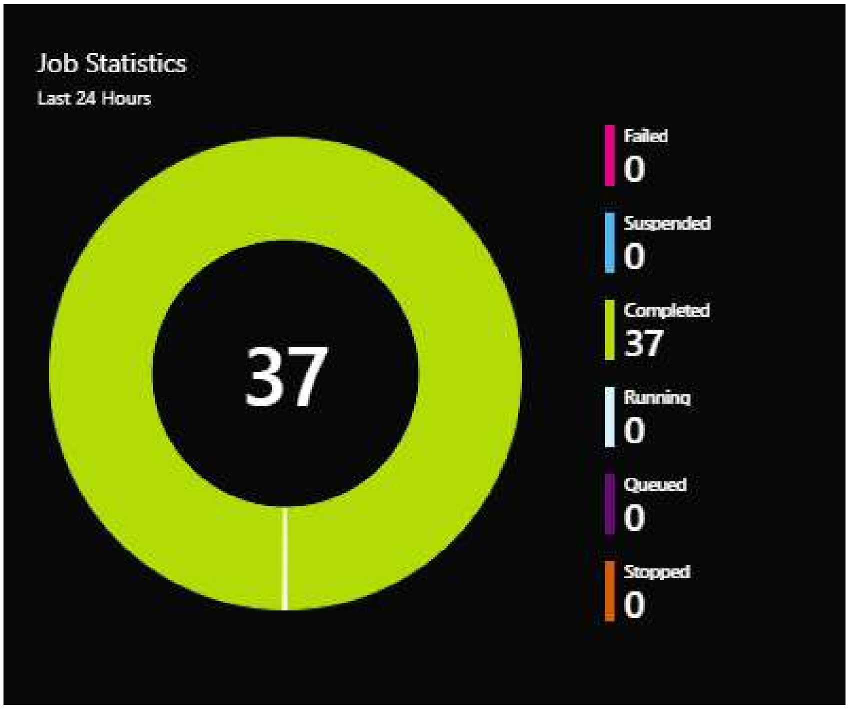
On these days
✓ Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday

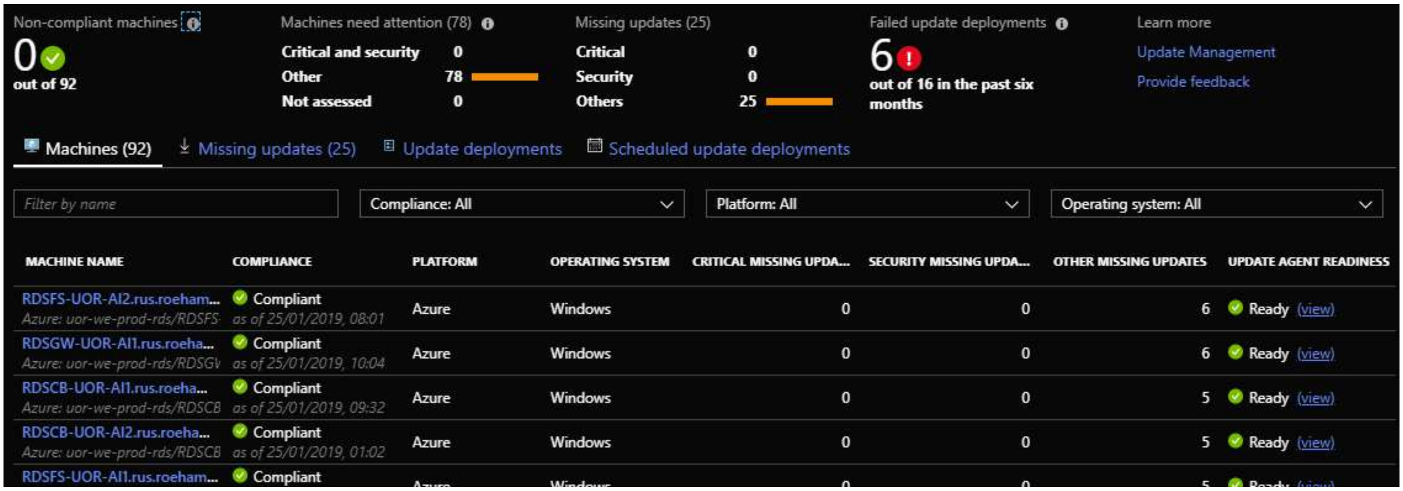
Set expiration
Yes [✓ No]

Expires
Never

# 7. Appendix 2 - Monitoring and Reporting

Systems managed in the University cloud environment will be monitored daily for compliance using Azure Automation – Update Management.





Non-compliant machines
0 ✓
out of 92

Machines need attention (78)

| | |
|---|---|
| Critical and security | 0 |
| Other | 78 |
| Not assessed | 0 |

Missing updates (25)

| | |
|---|---|
| Critical | 0 |
| Security | 0 |
| Others | 25 |

Failed update deployments
6 !
out of 16 in the past six months

Learn more
Update Management
Provide feedback

Machines (92) | Missing updates (25) | Update deployments | Scheduled update deployments

Filter by name
Compliance: All
Platform: All
Operating system: All

| MACHINE NAME | COMPLIANCE | PLATFORM | OPERATING SYSTEM | CRITICAL MISSING UPDA... | SECURITY MISSING UPDA... | OTHER MISSING UPDATES | UPDATE AGENT READINESS |
|---|---|---|---|---|---|---|---|
| RDSFS-UOR-AI2.rus.roeham...<br>Azure: uor-we-prod-rds/RDSFS | ✓ Compliant<br>as of 25/01/2019, 08:01 | Azure | Windows | 0 | 0 | 6 | ✓ Ready (view) |
| RDSGW-UOR-AI1.rus.roeha...<br>Azure: uor-we-prod-rds/RDSGV | ✓ Compliant<br>as of 25/01/2019, 10:04 | Azure | Windows | 0 | 0 | 6 | ✓ Ready (view) |
| RDSCB-UOR-AI1.rus.roeha...<br>Azure: uor-we-prod-rds/RDSCB | ✓ Compliant<br>as of 25/01/2019, 09:32 | Azure | Windows | 0 | 0 | 5 | ✓ Ready (view) |
| RDSCB-UOR-AI2.rus.roeha...<br>Azure: uor-we-prod-rds/RDSCB | ✓ Compliant<br>as of 25/01/2019, 01:02 | Azure | Windows | 0 | 0 | 5 | ✓ Ready (view) |
| RDSFS-UOR-AI1.rus.roeham... | ✓ Compliant | Azure | Windows | 0 | 0 | 5 | ✓ Ready (view) |